TECHNICAL
::: NOTE

Enabling BitLocker on the BIOFIRE® SPOTFIRE® Control Station

Contents

1. Introduction

Windows BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. BitLocker encrypts all user files and system files on the operating system drive.

bioMérieux has provided instructions on how to configure this **optional feature** on the Control Station in this Technical Note.

NOTE: While BitLocker is encrypting the data using this Technical Note, the SPOTFIRE System cannot perform any patient tests (this could be several hours depending on the amount of data on the hard drive). The control station must be kept ON during this process.

NOTE: It is the customer's responsibility to maintain the BitLocker recovery key. It is recommended to provide a copy of the key to the customer's IT department.

NOTE: BitLocker must be disabled prior to the system being returned for a service event. See Section 6 for instructions on how to disable BitLocker.

2. Scope

This document is limited to the SPOTFIRE System.

3. What's Needed?

- USB drive
- USB keyboard
- Password for LabAdmin account
- Expect the process to take a few hours (dependent on amount of data)
- No tests should be in progress

4. How to Configure BitLocker (C: Drive)

1. Plug in a USB keyboard to the Control Station.
2. From SPOTFIRE Application, press **CTRL + ALT + DEL** , and Select **Sign Off.**
3. Log into **LabAdmin**
4. From the Windows 10 Menu, search and then open **Manage BitLocker** (*Figure* 1)

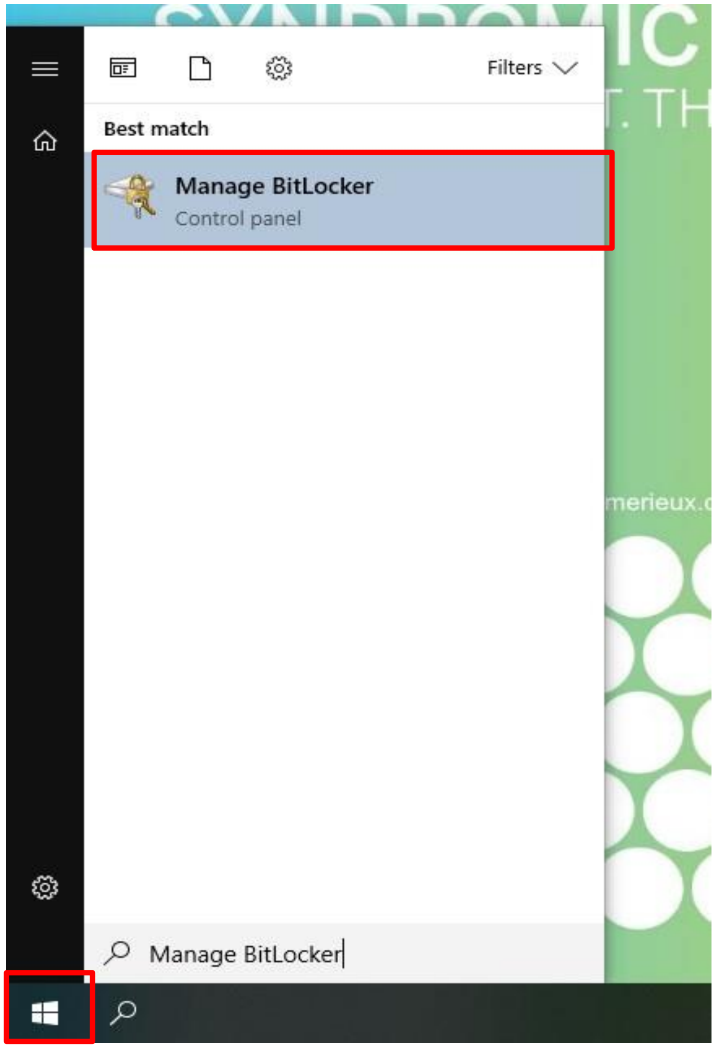
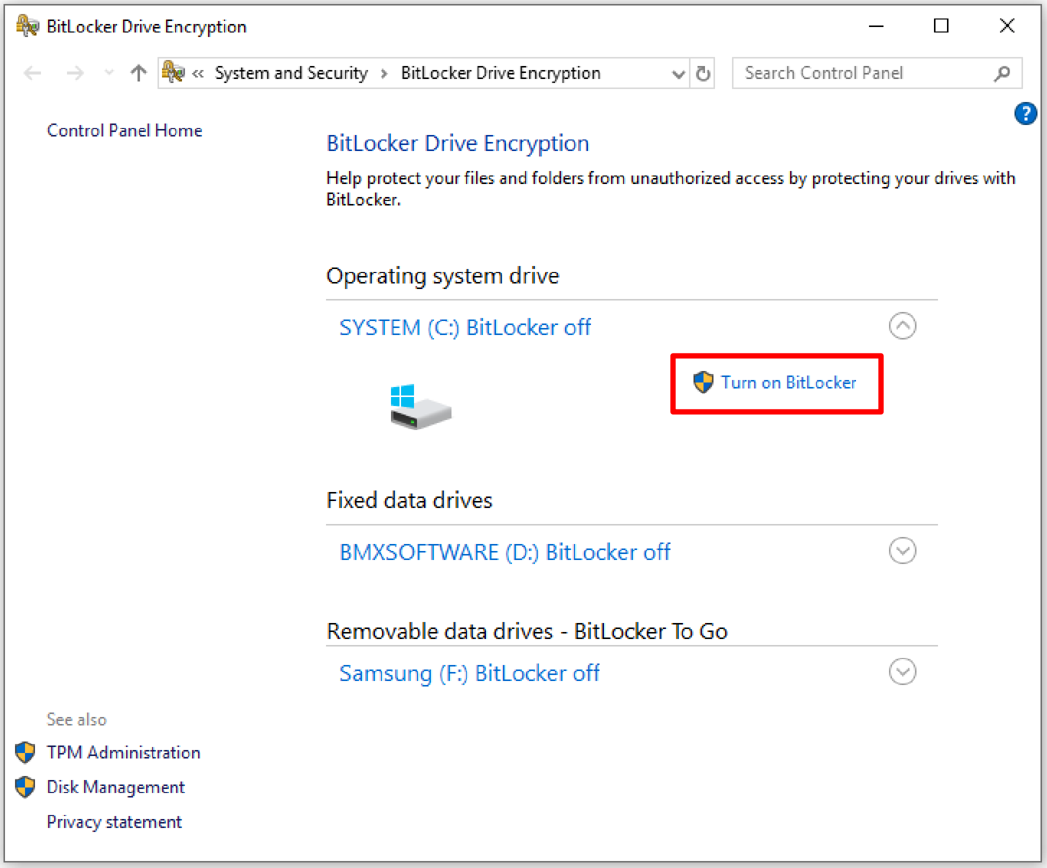


Figure 1

5. Turn on BitLocker for C: Drive
    a. The BitLocker Encryption Wizard will pop up, follow the Wizard steps to enable BitLocker (*Figures* 2 through 7).



BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

SYSTEM (C:) BitLocker off

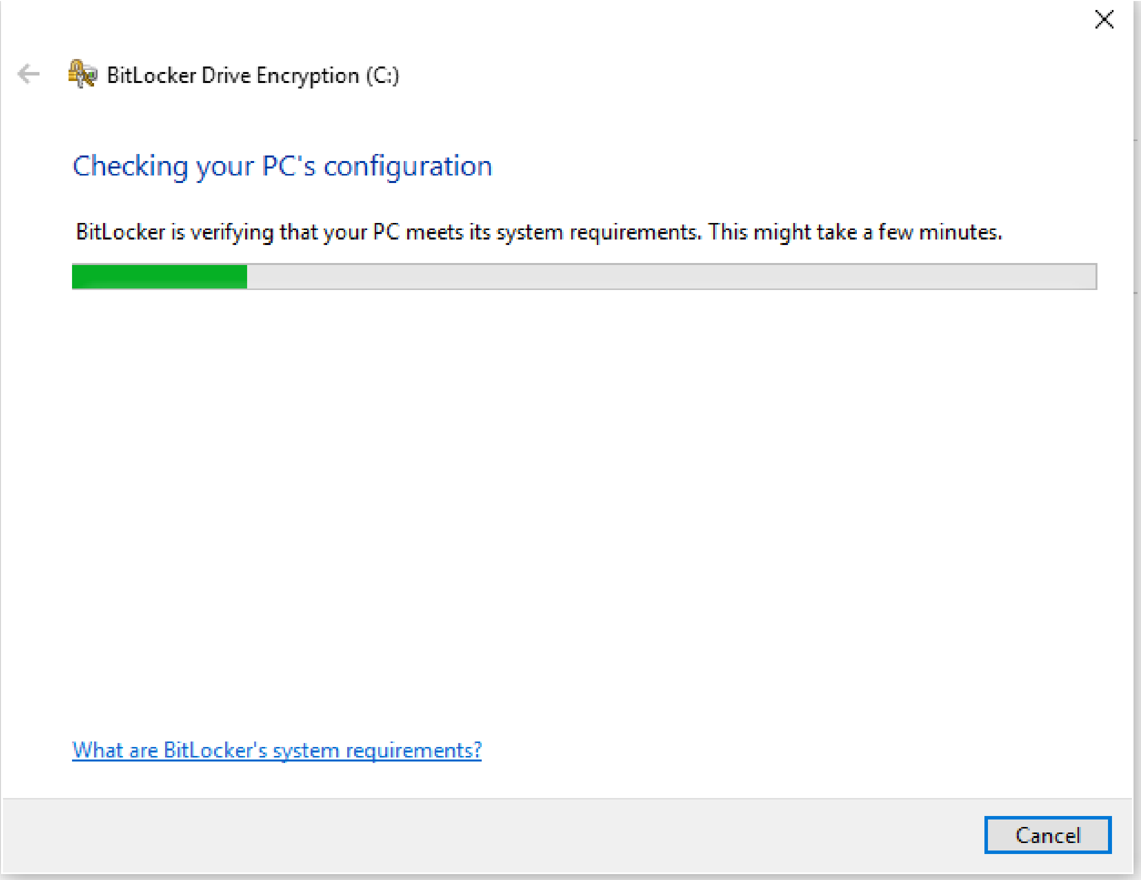
Fixed data drives

BMXSOFTWARE (D:) BitLocker off

Removable data drives - BitLocker To Go

Samsung (F:) BitLocker off

Figure 2



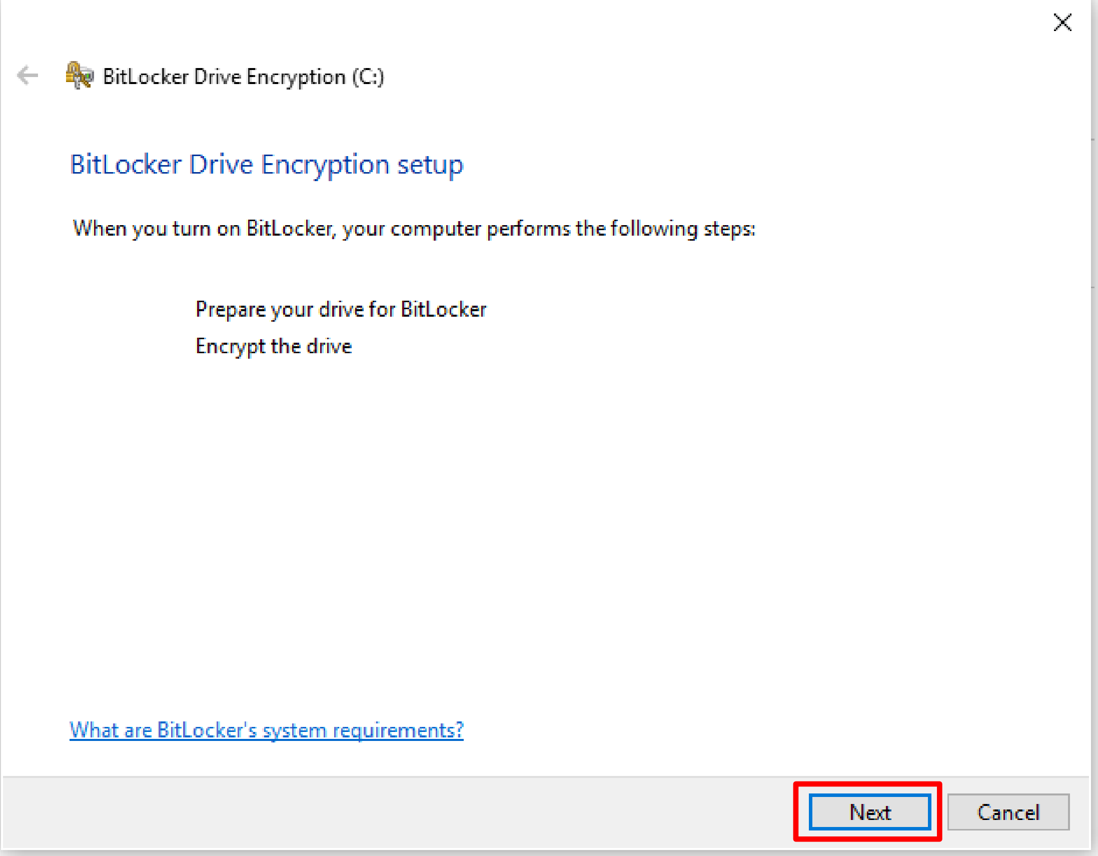
BitLocker Drive Encryption (C:)

Checking your PC's configuration

BitLocker is verifying that your PC meets its system requirements. This might take a few minutes.

What are BitLocker's system requirements?

Figure 3



BitLocker Drive Encryption (C:)

BitLocker Drive Encryption setup

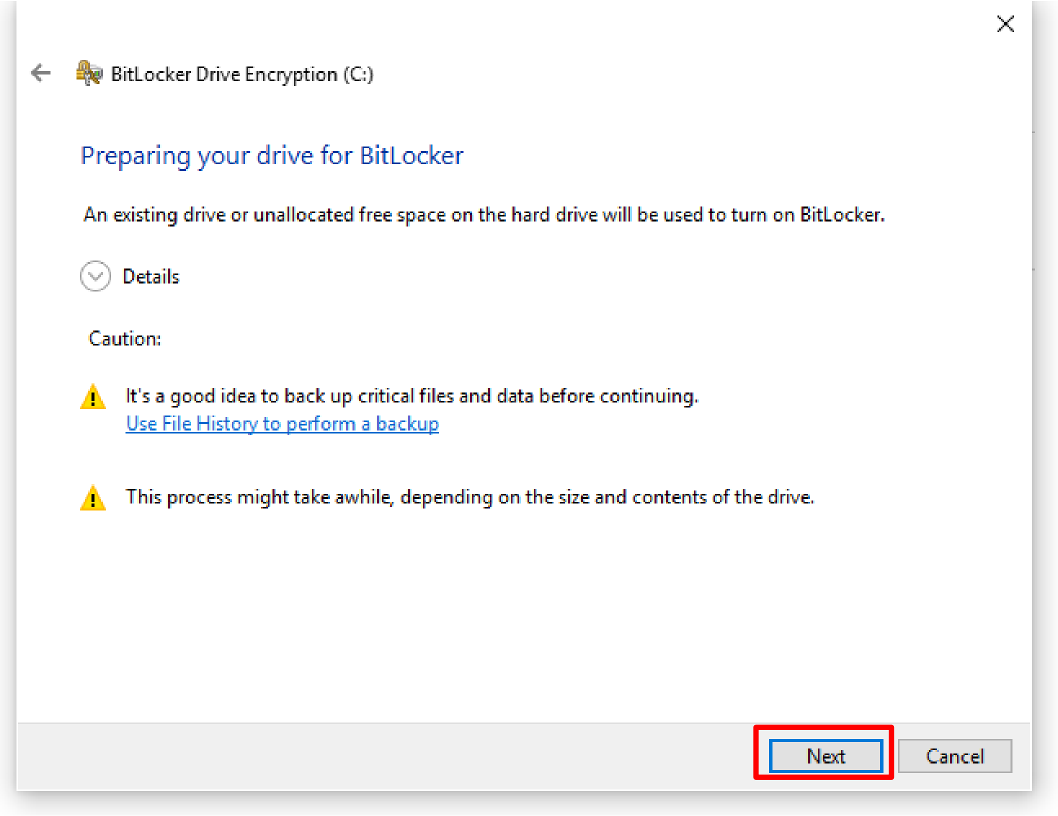
When you turn on BitLocker, your computer performs the following steps:

Prepare your drive for BitLocker

Encrypt the drive

What are BitLocker's system requirements?

Figure 4



BitLocker Drive Encryption (C:)

Preparing your drive for BitLocker

An existing drive or unallocated free space on the hard drive will be used to turn on BitLocker.

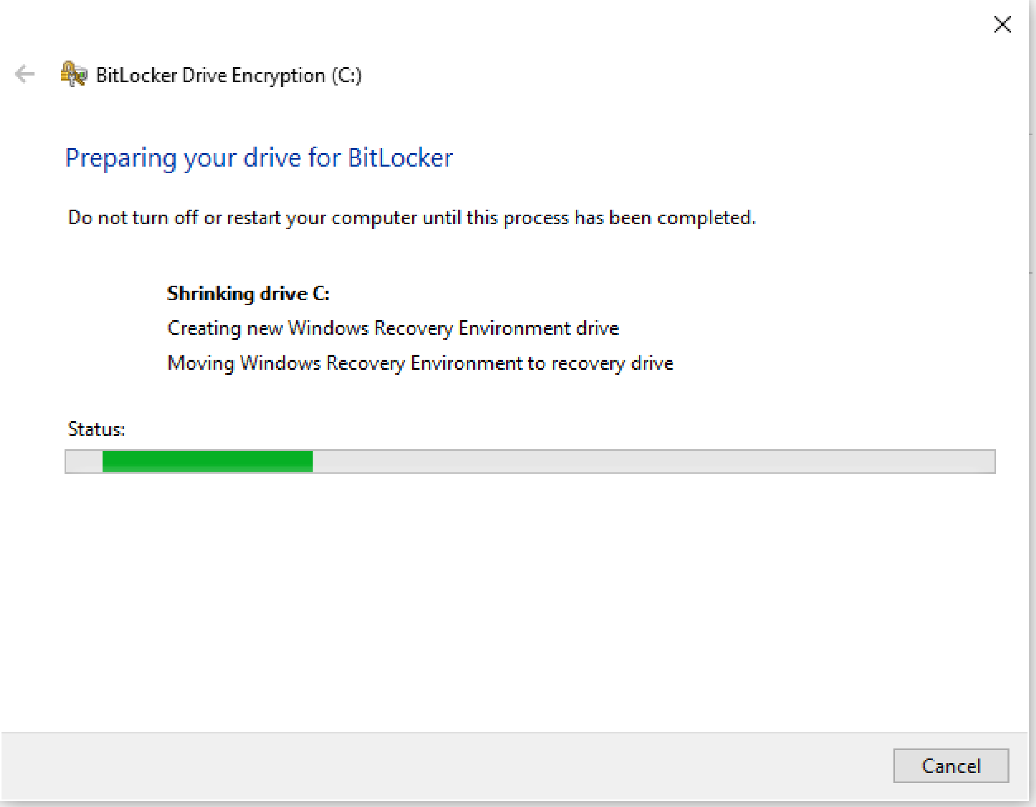
Details

Caution:

⚠ It's a good idea to back up critical files and data before continuing.
Use File History to perform a backup

⚠ This process might take awhile, depending on the size and contents of the drive.

Figure 5



BitLocker Drive Encryption (C:)

Preparing your drive for BitLocker

Do not turn off or restart your computer until this process has been completed.

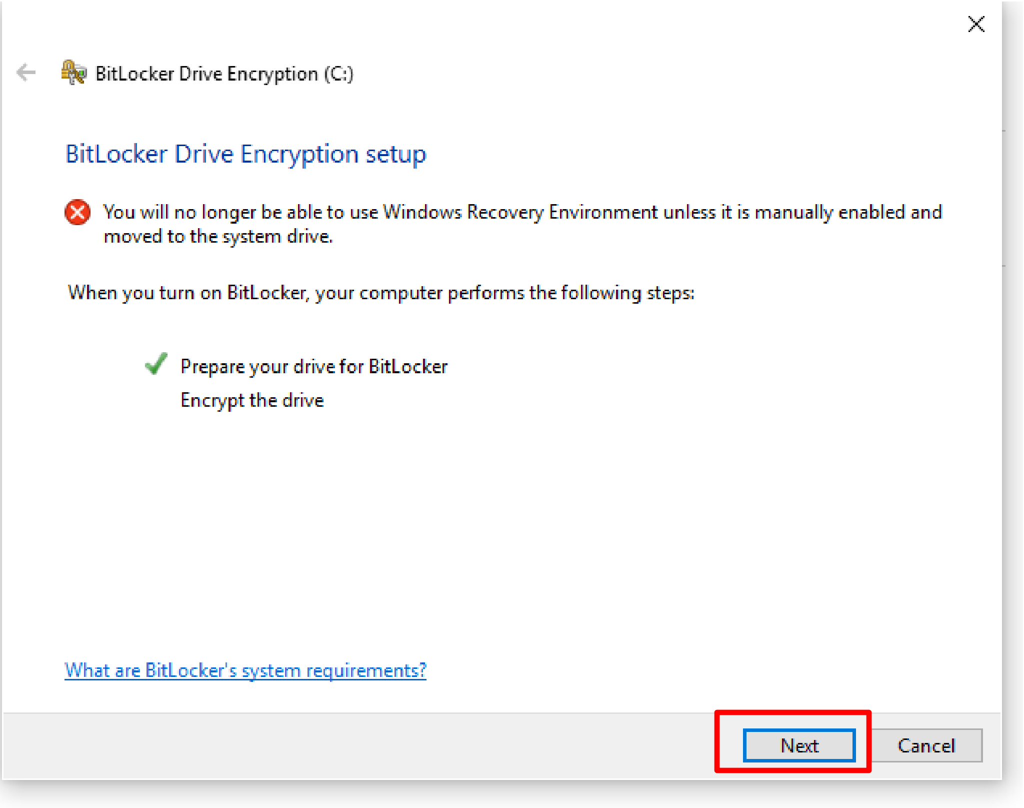
Shrinking drive C:

Creating new Windows Recovery Environment drive

Moving Windows Recovery Environment to recovery drive

Status:

Figure 6



BitLocker Drive Encryption (C:)

BitLocker Drive Encryption setup

You will no longer be able to use Windows Recovery Environment unless it is manually enabled and moved to the system drive.

When you turn on BitLocker, your computer performs the following steps:

✓ Prepare your drive for BitLocker

Encrypt the drive

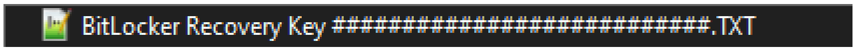
What are BitLocker's system requirements?

Figure 7

6. Insert a USB into the Control Station. Once plugged in, select **Save to a File** (*Figure* 8).

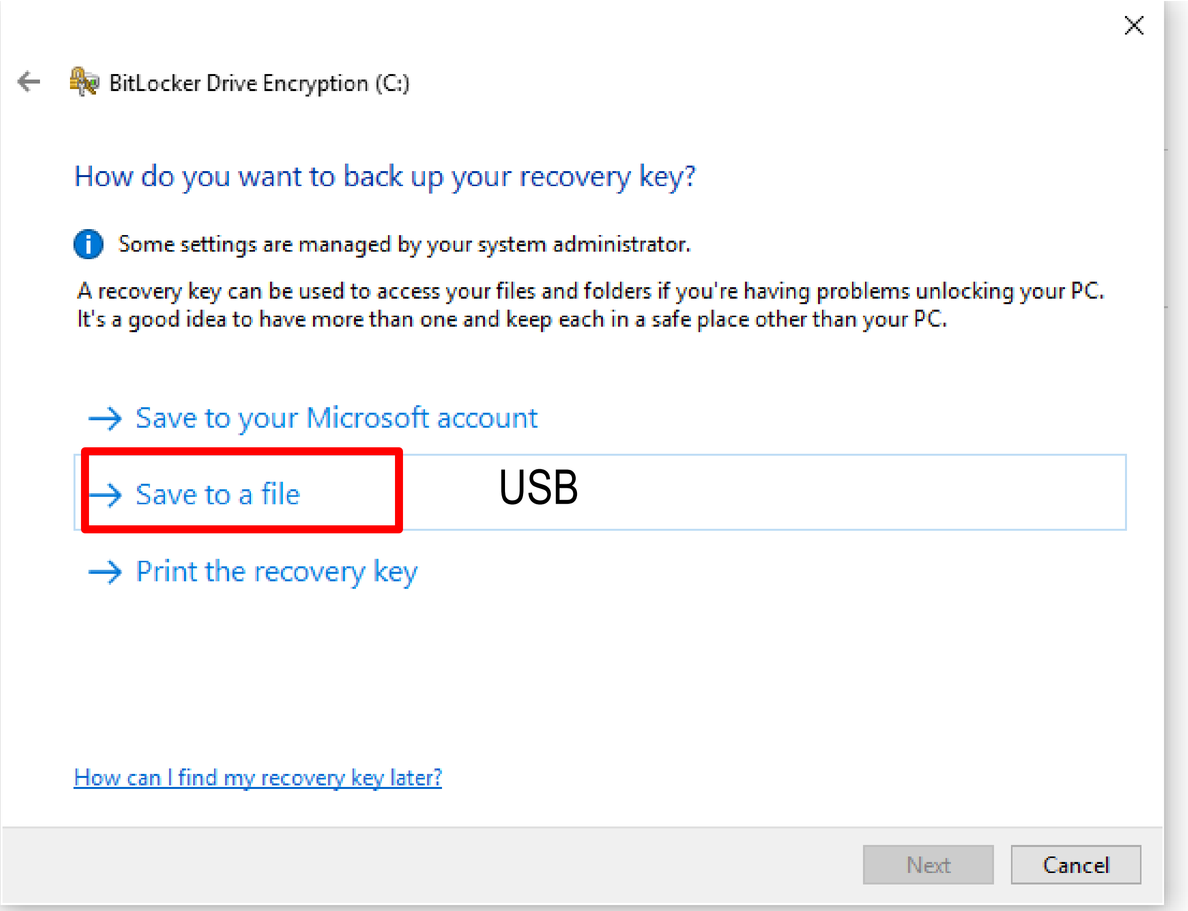
7. The Windows Explorer Window will pop up, select the USB you have inserted in the system to save your recovery key. Ensure the USB drive is labeled and tracked.

NOTE: This recovery key is vital once BitLocker is enabled if the customer is locked out of the system. Please note it is the customer's responsibility to maintain this key.



BitLocker Recovery Key ###################################.TXT

NOTE: BitLocker Recovery Key will look similar to the above image once saved to a USB, hashes will be your direct recovery key.



BitLocker Drive Encryption (C:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

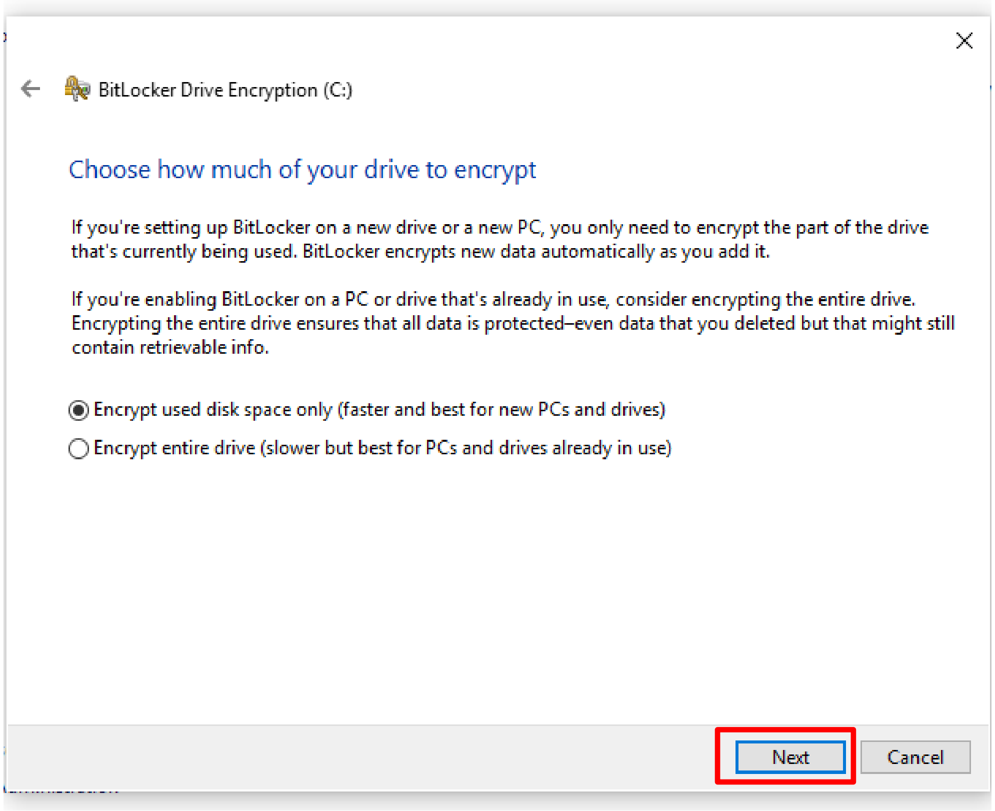
→ Save to your Microsoft account
→ Save to a file
USB
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel

Figure 8

8. Choose how much of the drive to encrypt and Select **Next** (*Figure* 9).

   a. **Brand new system:** Encrypt used disk space only, all new data will be encrypted as it's written to the disk. This is expected to take 20-30min.

   b. **Older system with test data:** Encrypt entire drive, all new data will be encrypted as it's written to the disk. This is expected to take a few hours depending on how much data is on the disk.



BitLocker Drive Encryption (C:)

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.

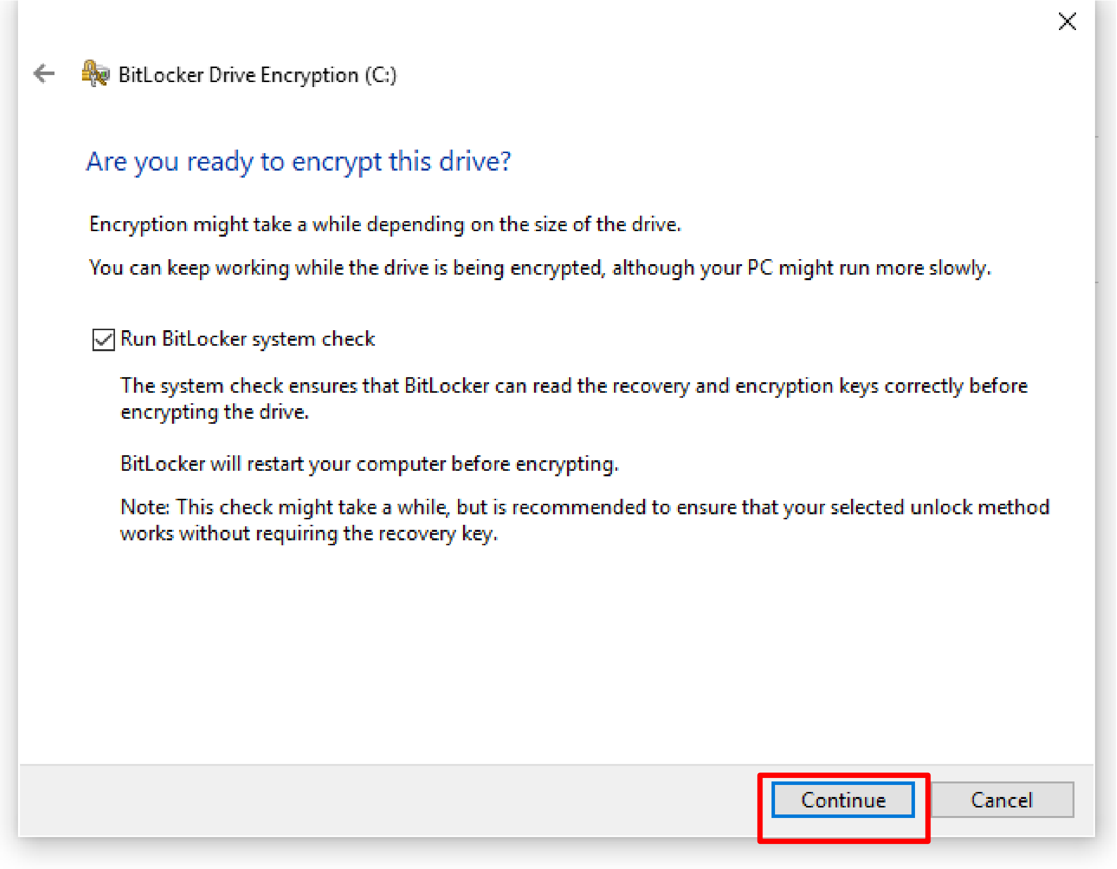
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

● 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)

Figure 9

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



BitLocker Drive Encryption (C:)

Are you ready to encrypt this drive?

Encryption might take a while depending on the size of the drive.

You can keep working while the drive is being encrypted, although your PC might run more slowly.

☑ Run BitLocker system check

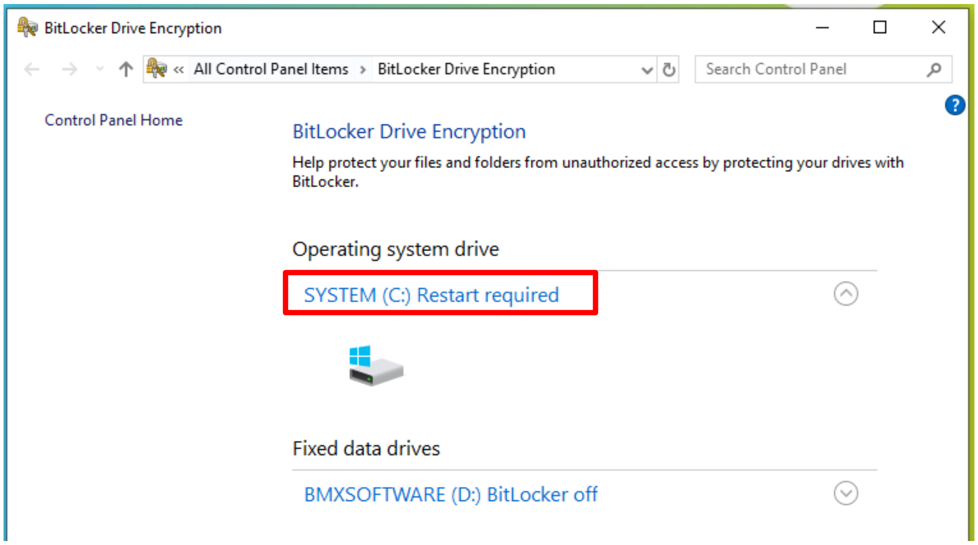
The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

BitLocker will restart your computer before encrypting.

Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.

Figure 10

10. After BitLocker Encryption is complete, Restart the System to complete setup and return to the SPOTFIRE Software (*Figure* 11).



BitLocker Drive Encryption

« All Control Panel Items › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

SYSTEM (C:) Restart required

Fixed data drives

BMXSOFTWARE (D:) BitLocker off

Figure 11

11. Restart System by navigating to the **Windows logo→ Power icon → Restart** (*Figure* 12).

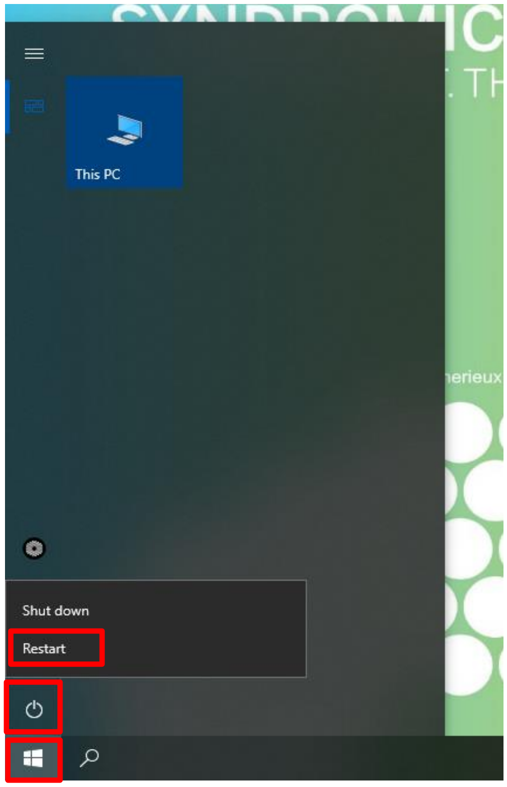


Figure 12

5. How to Configure BitLocker on BMXSOFTWARE (D: Drive)

1. Plug in a USB keyboard to the Control Station.
2. From SPOTFIRE Application, press **CTRL + ALT + DEL** , and Select Sign Off.
3. Log into **LabAdmin**
4. From the Windows 10 Menu, search and then open **Manage BitLocker** (*Figure* 13)

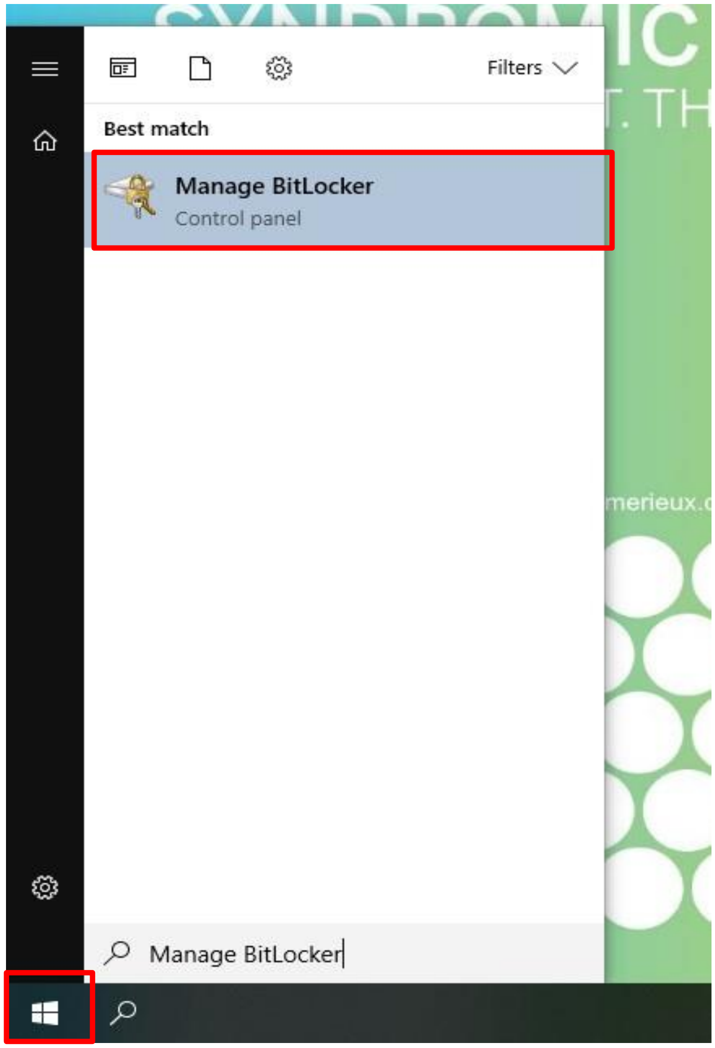
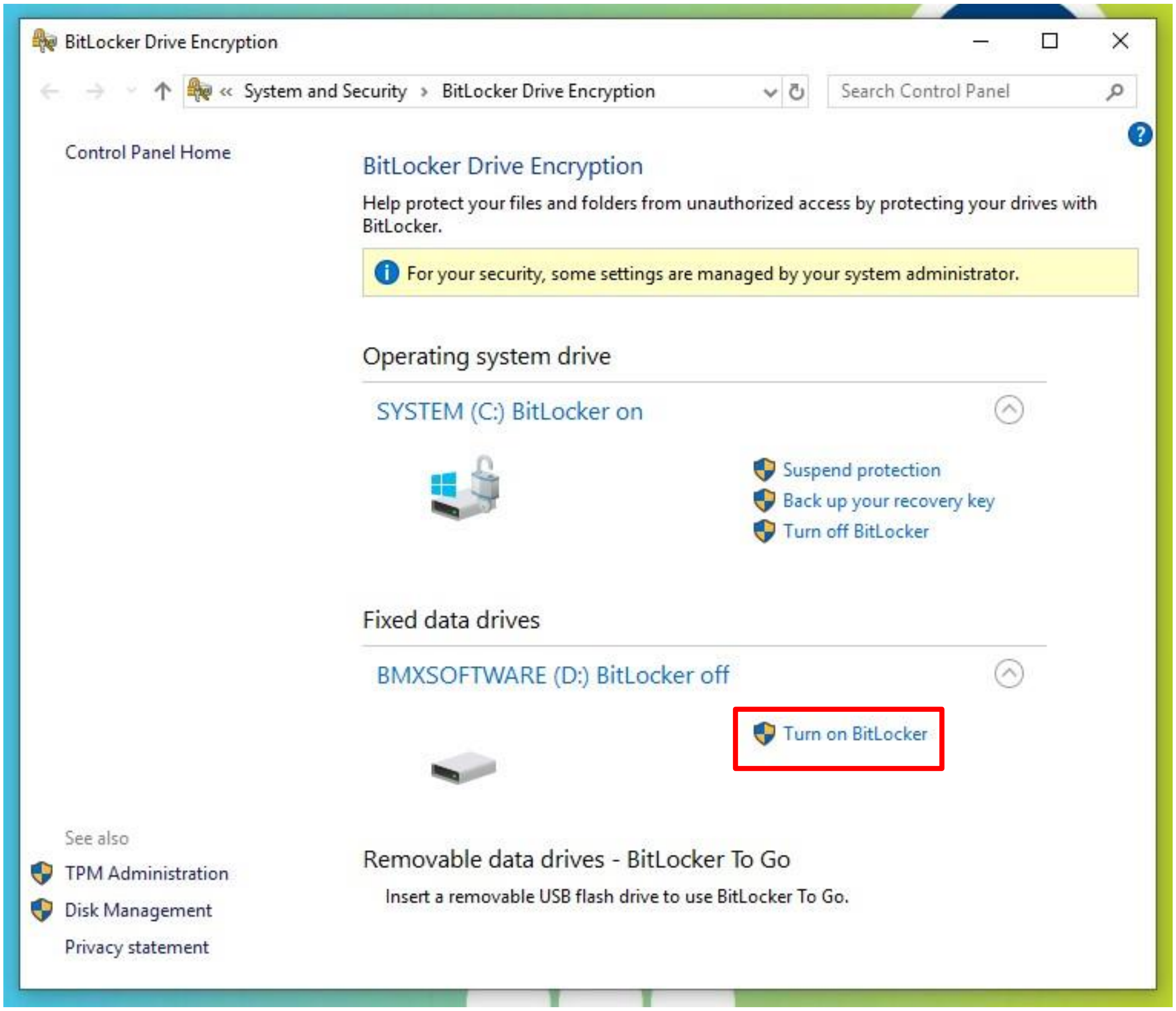


Figure 13

5. Select **Turn on BitLocker** for D: Drive (*Figure* 14).



BitLocker Drive Encryption
« System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

SYSTEM (C:) BitLocker on

Suspend protection
Back up your recovery key
Turn off BitLocker

Fixed data drives

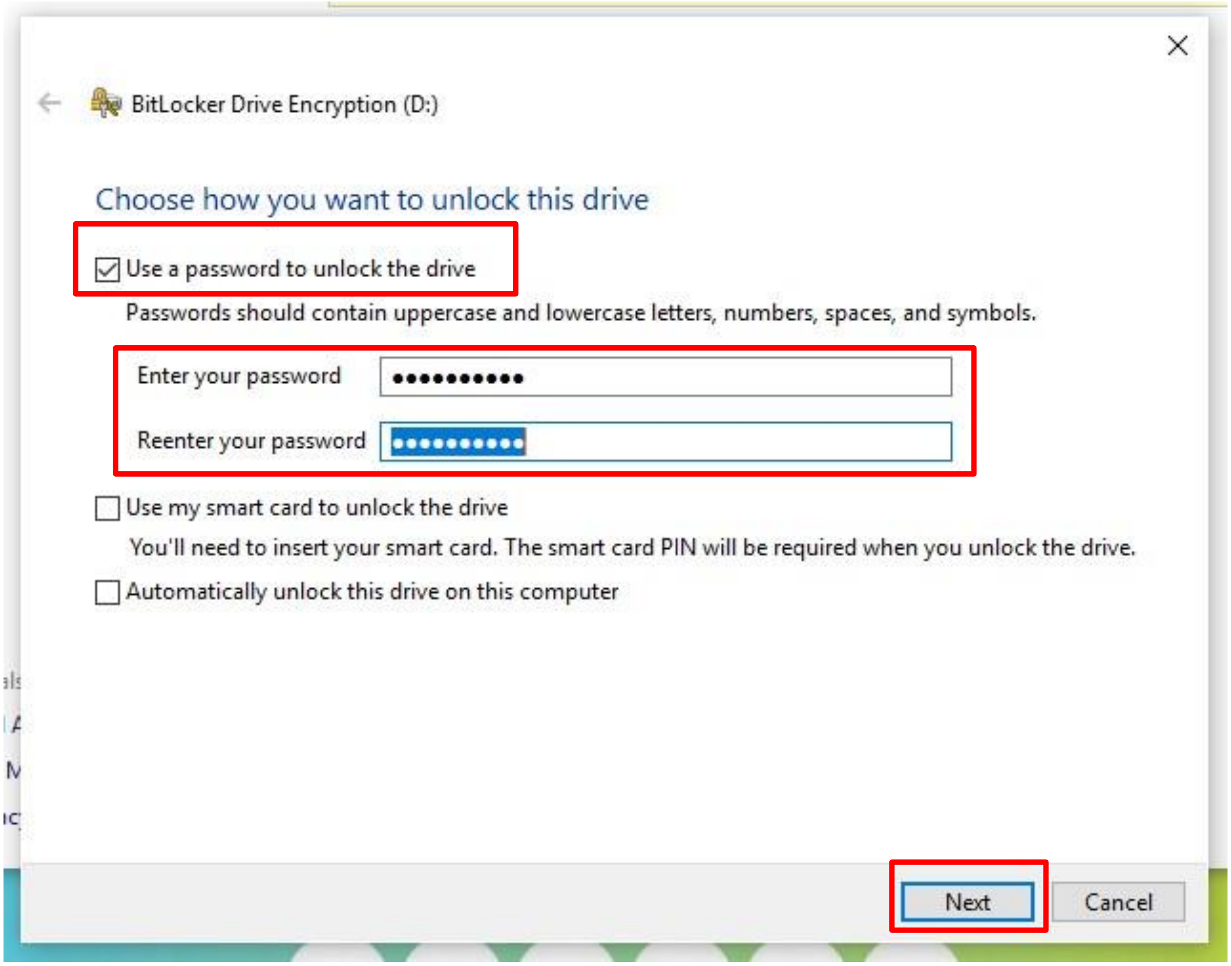
BMXSOFTWARE (D:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

Figure 14

6. Choose how you want to unlock the D: Drive by selecting the checkbox “**Use a password to unlock the drive**” and entering a **password** and selecting **Next** (*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.

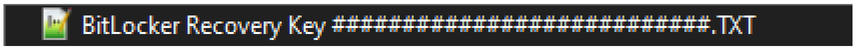
□ Automatically unlock this drive on this computer

Figure 15

7. Insert a USB into the Control Station. Once plugged in, select **Save to a USB flash drive** (*Figure* 16).

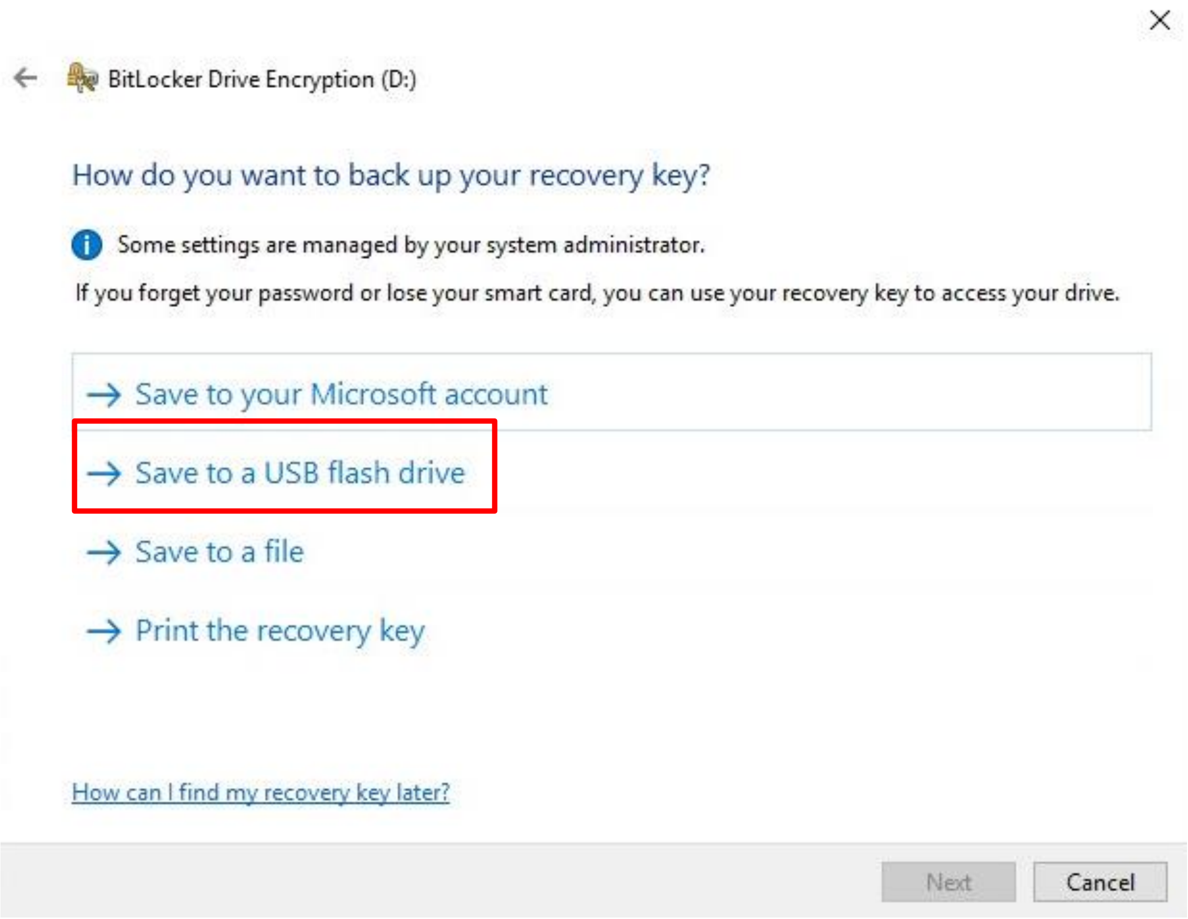
8. The Windows Explorer Window will pop up, select the USB you have inserted in the system to save your recovery key. Ensure the USB drive is labeled and tracked.

NOTE: This recovery key is vital once BitLocker is enabled if the customer is locked out of the system. Please note it is the customer's responsibility to maintain this key.



BitLocker Recovery Key ###########################.TXT

NOTE: BitLocker Recovery Key will look similar to the above image once saved to a USB, hashes will be your direct recovery key.



BitLocker Drive Encryption (D:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

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

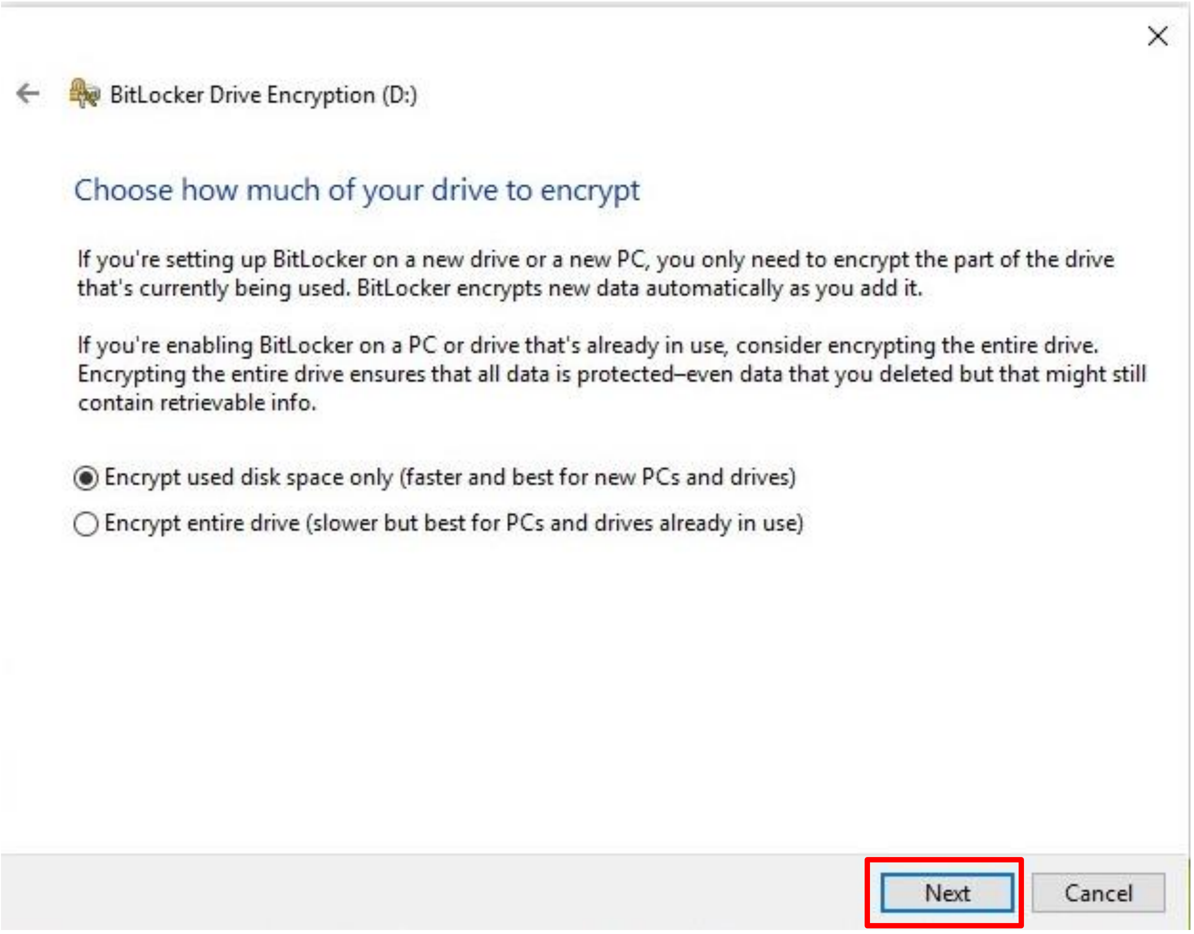
→ Save to your Microsoft account
→ Save to a USB flash drive
→ Save to a file
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel

Figure 16

9. Choose how much of the drive to encrypt then select **Next** (*Figure* 17)

   c. **Brand new system:** Encrypt used disk space only, all new data will be encrypted as it's written to the disk. This is expected to take 20-30min.

   d. **Older system with test data:** Encrypt entire drive, all new data will be encrypted as it's written to the disk. This is expected to take a few hours depending on how much data is on the disk.



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.

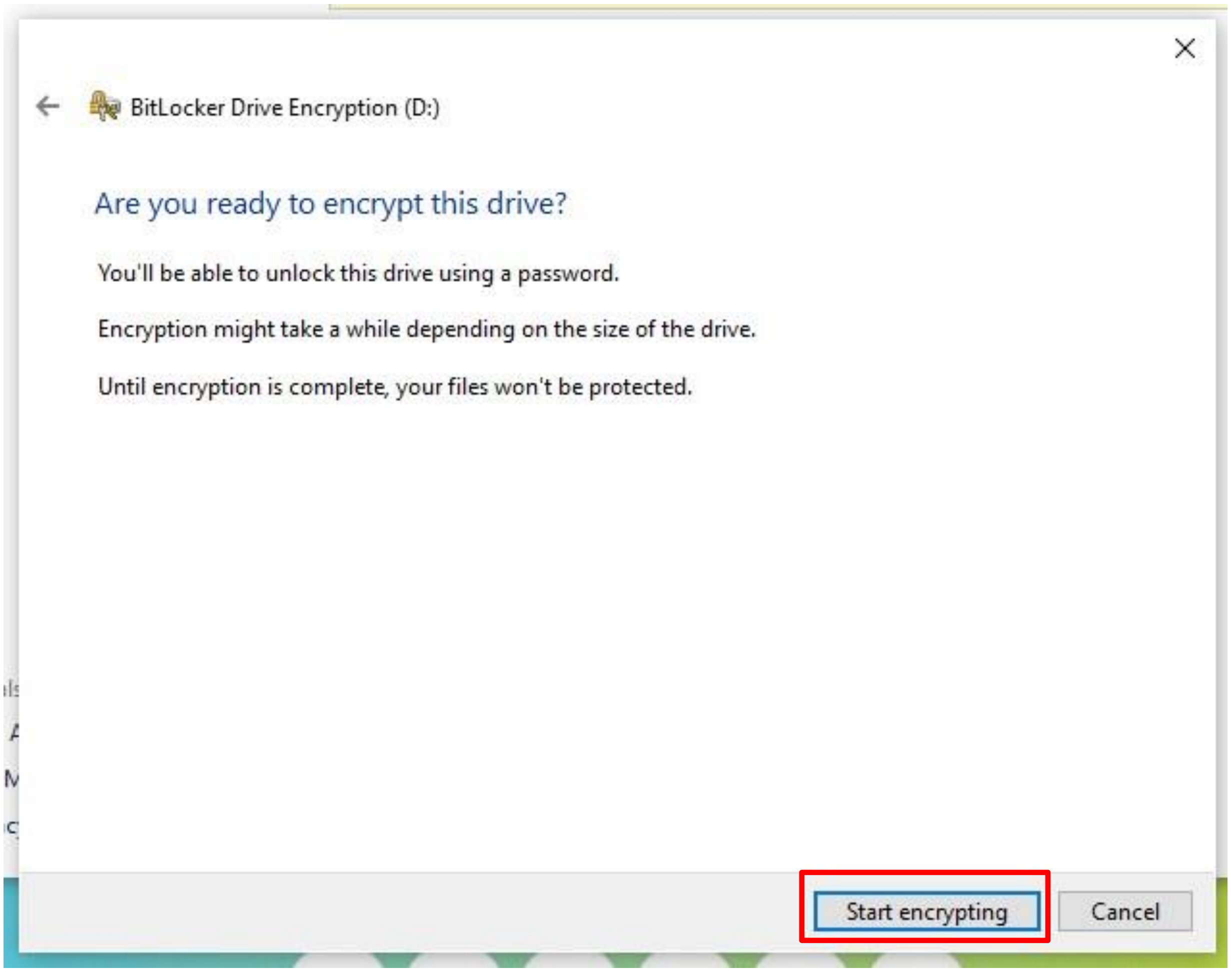
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

● 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)

Figure 17

10. Select **Start Encrypting** the D: Drive (*Figure* 18).



BitLocker Drive Encryption (D:)

Are you ready to encrypt this drive?

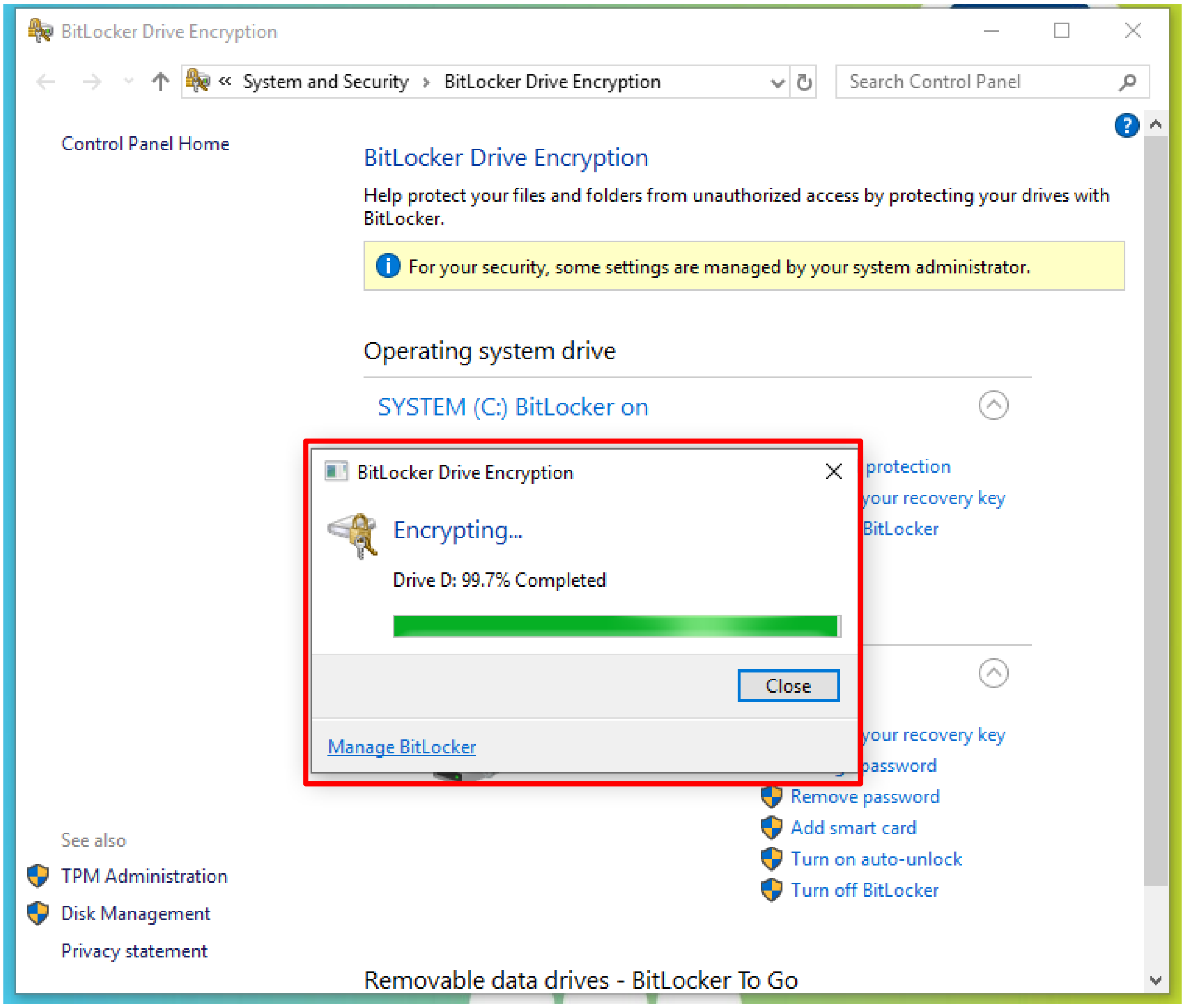
You'll be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

Figure 18

11. The progress of encryption is shown in *Figure* 19.



BitLocker Drive Encryption

System and Security › BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

SYSTEM (C:) BitLocker on

BitLocker Drive Encryption

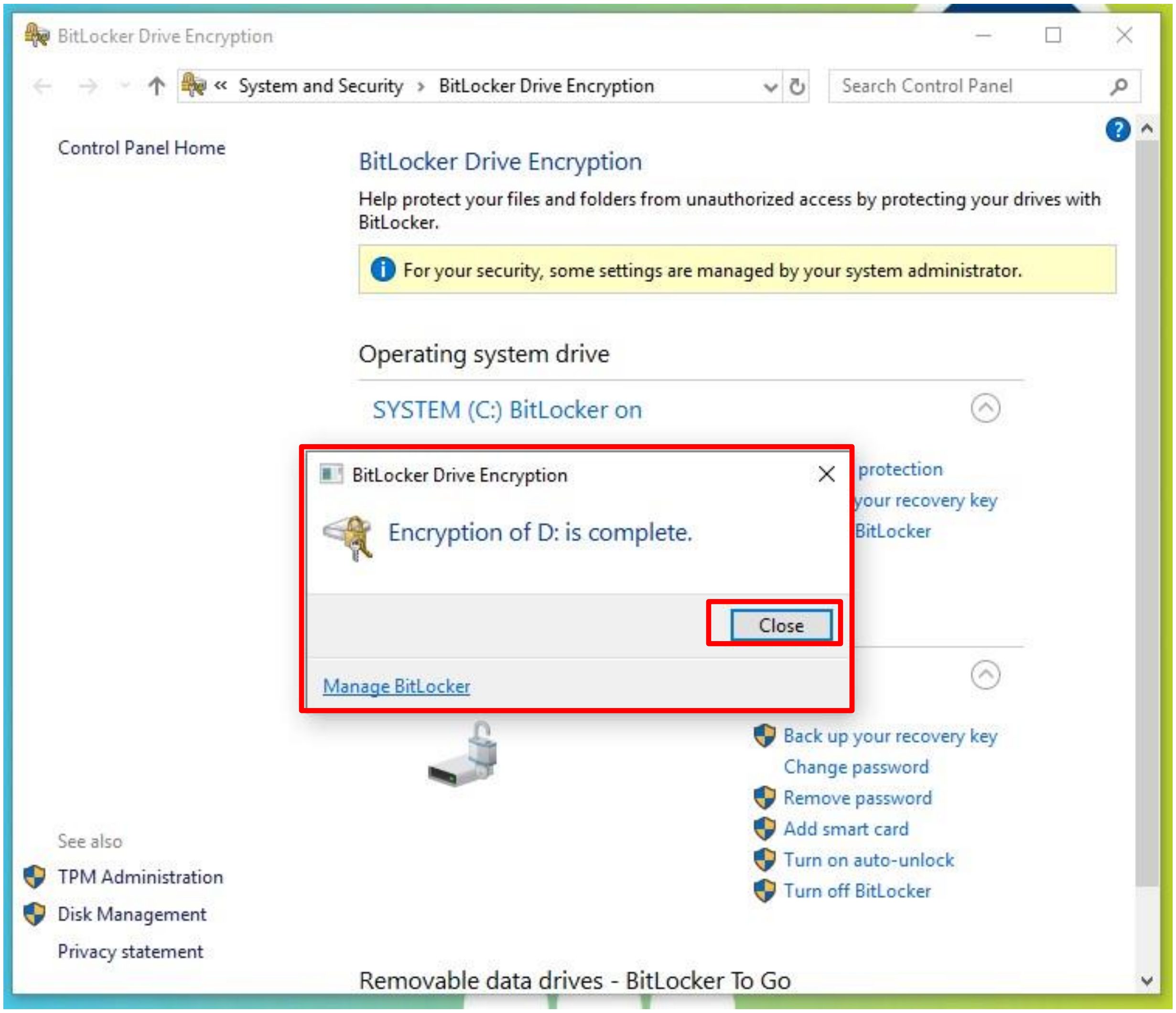
Encrypting...

Drive D: 99.7% Completed

Removable data drives - BitLocker To Go

Figure 19

12. Encryption of D: Drive is complete, select **Close** (*Figure* 20). *Figure* 21 confirms encryption of the D: Drive is complete.



BitLocker Drive Encryption

System and Security › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

SYSTEM (C:) BitLocker on

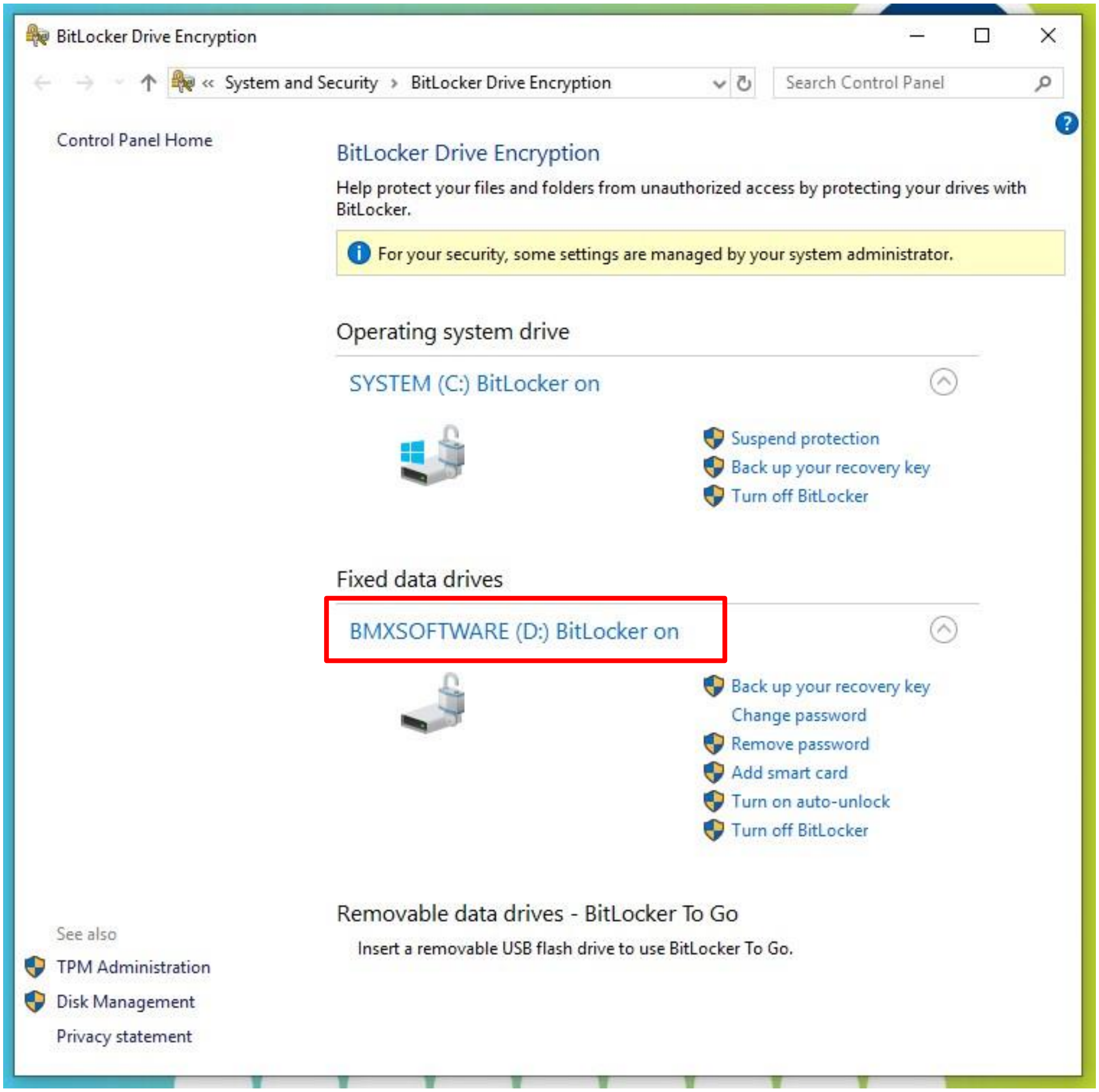
BitLocker Drive Encryption

Encryption of D: is complete.

Close

Manage BitLocker

Figure 20



BitLocker Drive Encryption

« System and Security › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

SYSTEM (C:) BitLocker on

- Suspend protection
- Back up your recovery key
- Turn off BitLocker

Fixed data drives

BMXSOFTWARE (D:) BitLocker on

- Back up your recovery key
- Change password
- Remove password
- Add smart card
- Turn on auto-unlock
- Turn off BitLocker

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

- TPM Administration
- Disk Management
- Privacy statement

Figure 21

13. After D: Drive BitLocker Encryption is complete, Restart the System to complete setup and return to the SPOTFIRE Software by navigating to the **Windows logo→ Power icon → Restart** (*Figure* 22).

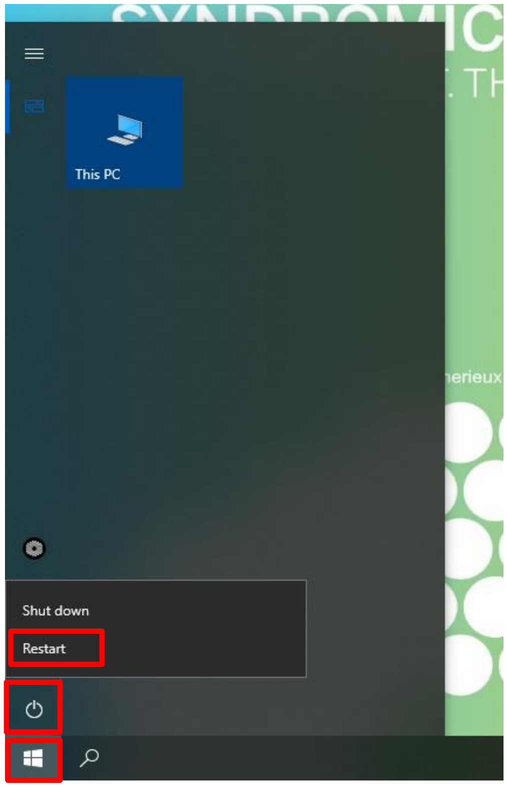


Figure 22

6. Disabling BitLocker

BitLocker will need to be disabled prior to the system being sent to Service.

NOTE: **Recovery Key is not required for decryption.**

6.1 Disabling BitLocker on C: Drive

1. Plug in a USB keyboard to the Control Station.
2. From SPOTFIRE Application, press **CTRL + ALT + DEL** , and Select Sign Off.
3. Log into **LabAdmin**
4. From the Windows 10 Menu, search and then open **Manage BitLocker** (*Figure* 23)

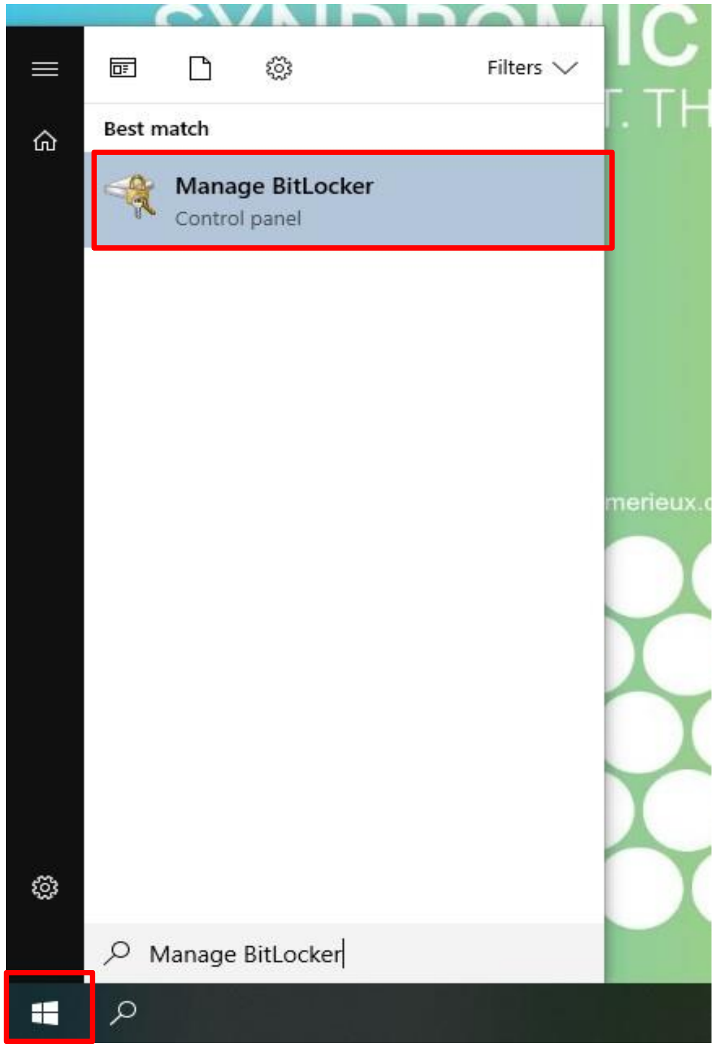
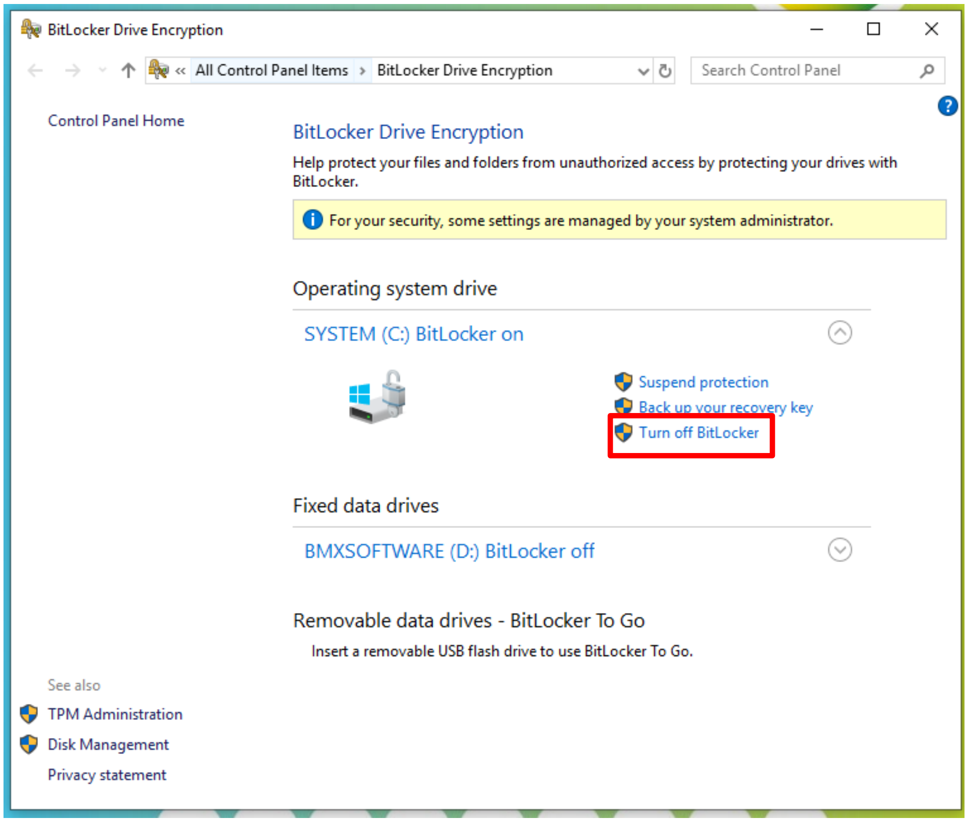


Figure 23

5. Select **Turn off BitLocker** (*Figure* 24).



BitLocker Drive Encryption

All Control Panel Items › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

SYSTEM (C:) BitLocker on

Suspend protection

Back up your recovery key

Turn off BitLocker

Fixed data drives

BMXSOFTWARE (D:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

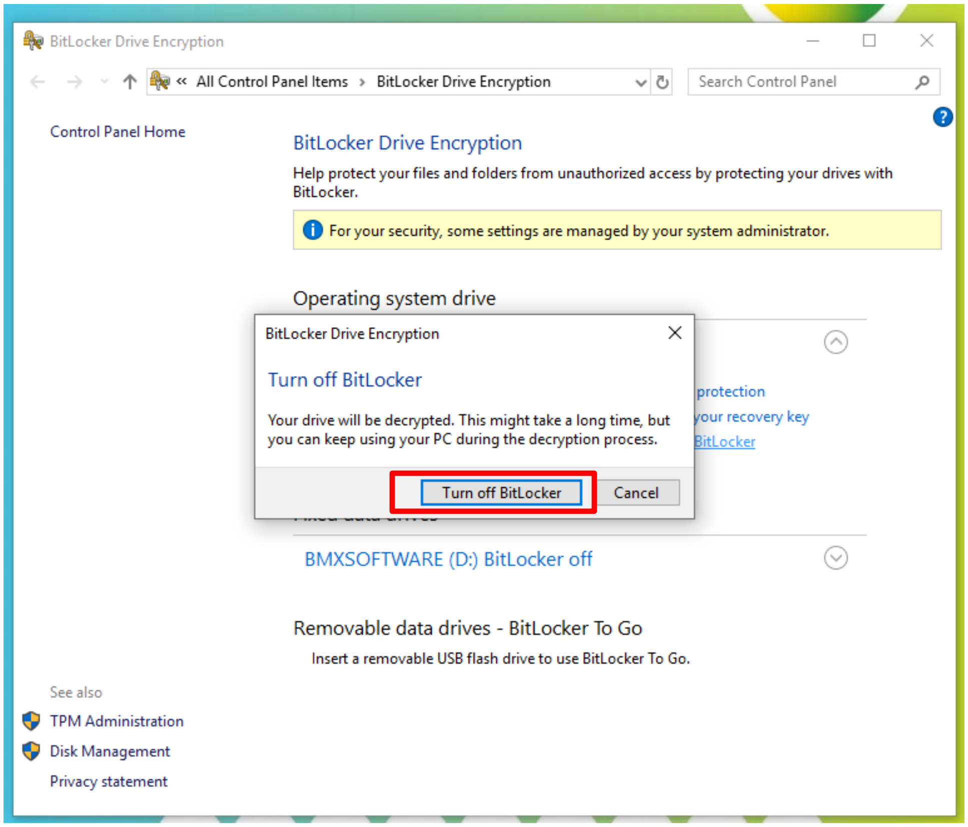
TPM Administration

Disk Management

Privacy statement

Figure 24

6. Confirmation prompt will pop up, confirm you want to **Turn off BitLocker** (*Figure* 25).



BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

BitLocker Drive Encryption

Turn off BitLocker

Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

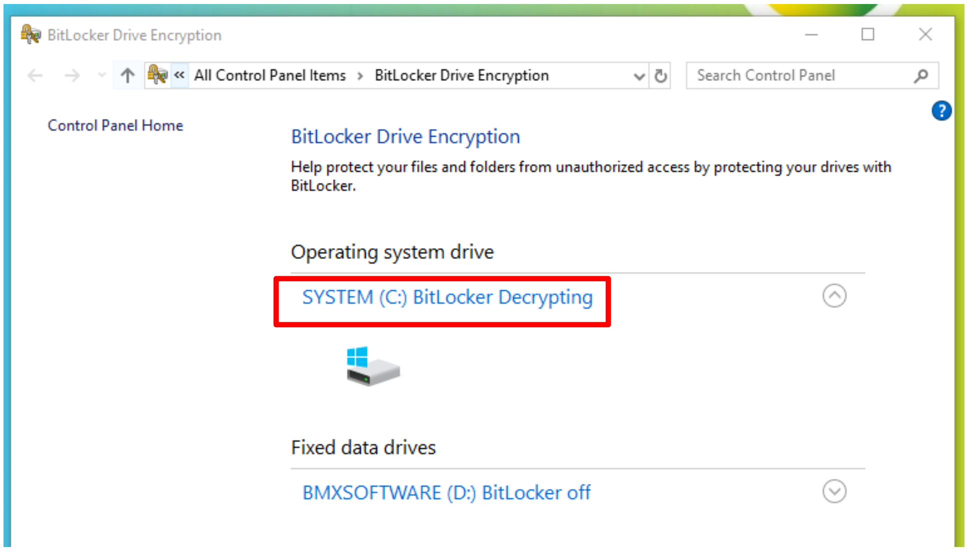
BMXSOFTWARE (D:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

Figure 25

7. Wait for BitLocker to Decrypt the C: Drive (*Figure* 26 and *Figure* 27)


BitLocker Drive Encryption

All Control Panel Items › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

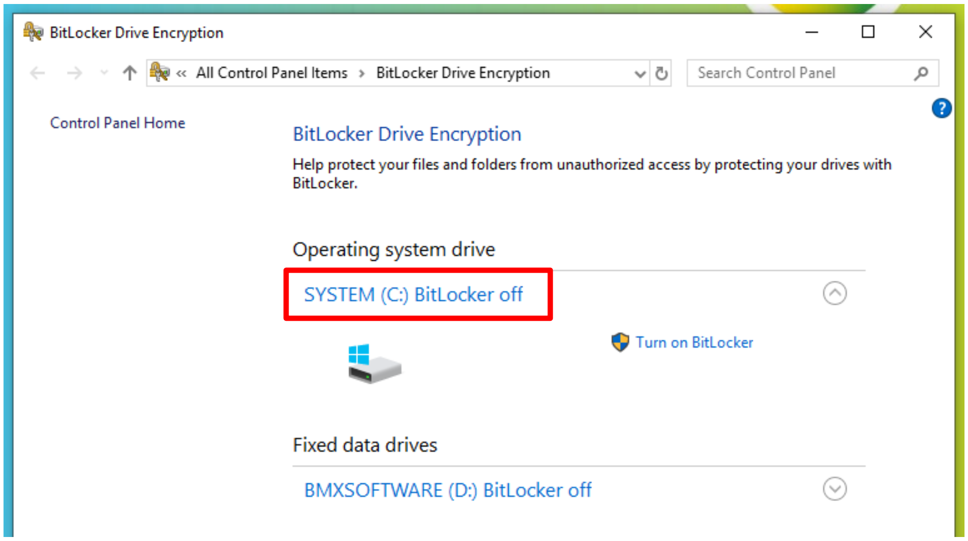
Operating system drive

SYSTEM (C:) BitLocker Decrypting

Fixed data drives

BMXSOFTWARE (D:) BitLocker off

Figure 26


BitLocker Drive Encryption

All Control Panel Items › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

SYSTEM (C:) BitLocker off

Turn on BitLocker

Fixed data drives

BMXSOFTWARE (D:) BitLocker off

Figure 27

8. Once Decryption is complete, Restart the System to complete setup and return to the SPOTFIRE Software. Navigate to **Windows Start Menu → Power →Restart** (*Figure* 28).

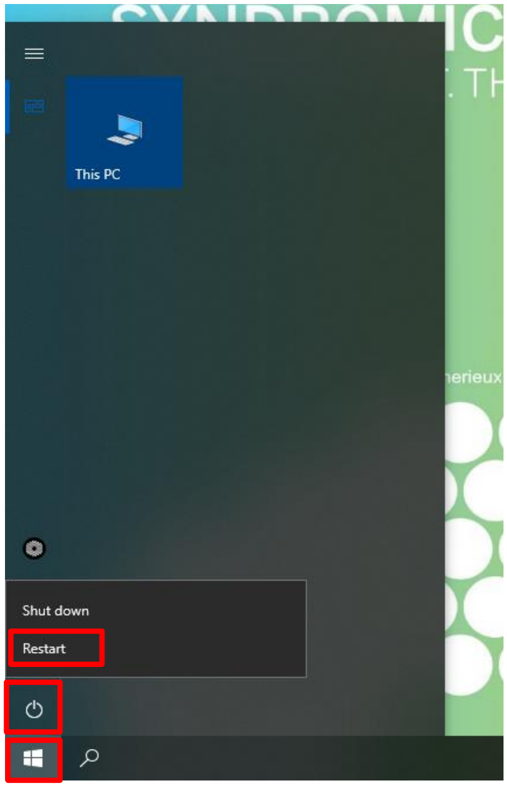


Figure 28

6.2 Disabling BitLocker on D: Drive

1. Plug in a USB keyboard to the Control Station.
2. From SPOTFIRE Application, press **CTRL + ALT + DEL** , and Select Sign Off.
3. Log into **LabAdmin**
4. From the Windows 10 Menu, search and then open **Manage BitLocker** (*Figure* 29)

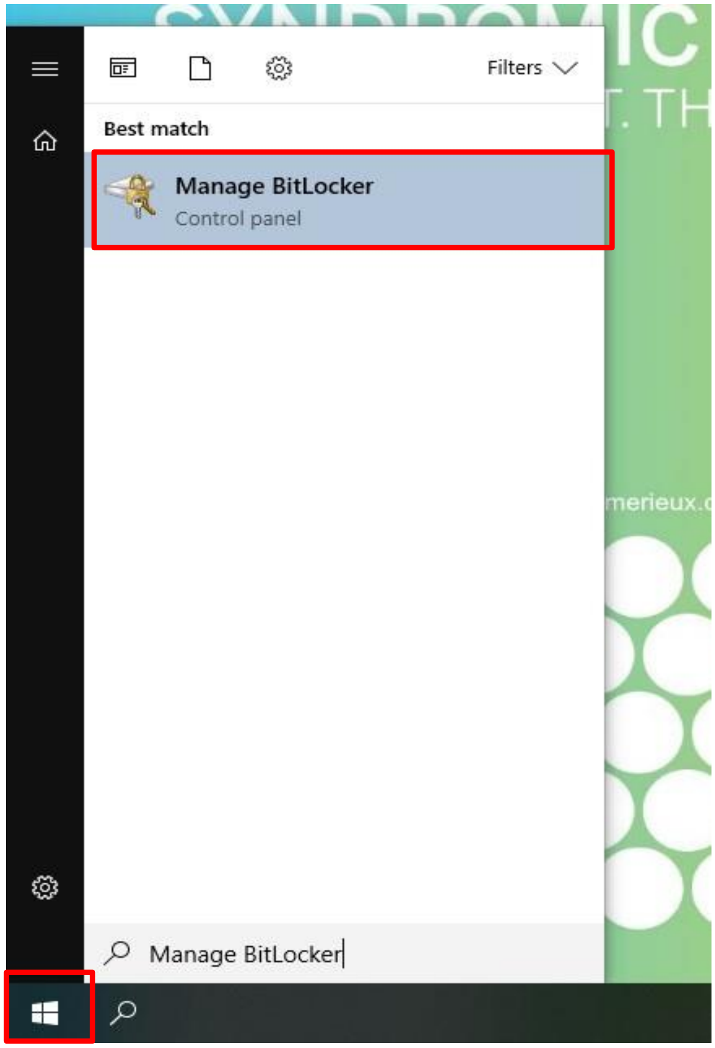
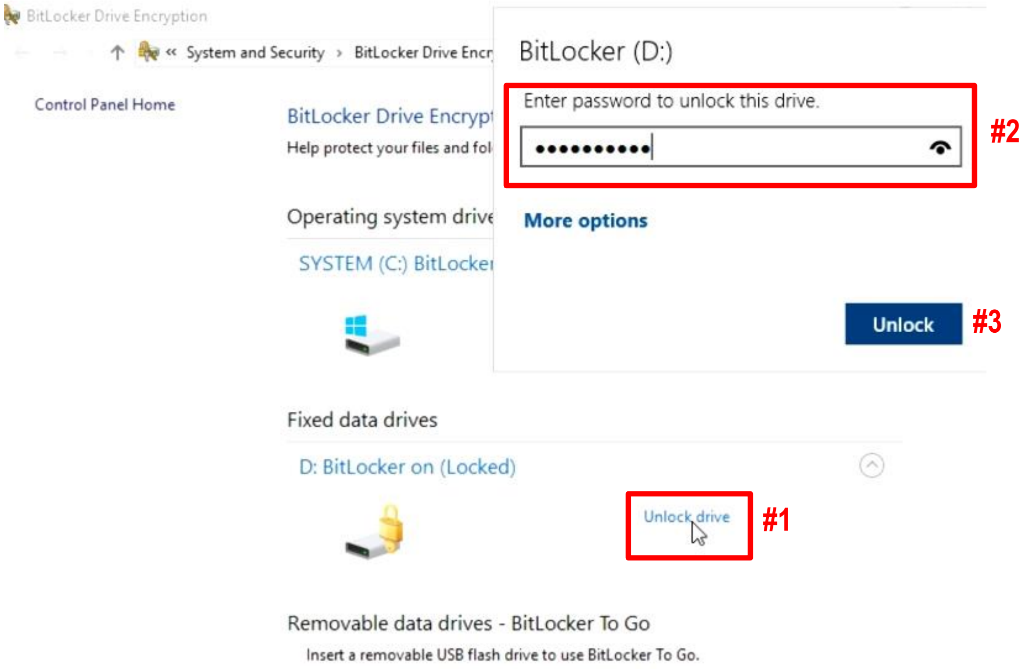


Figure 29

5. Select **Unlock drive,** Enter the password to unlock the drive, and select **Unlock.** (*Figure* 30)



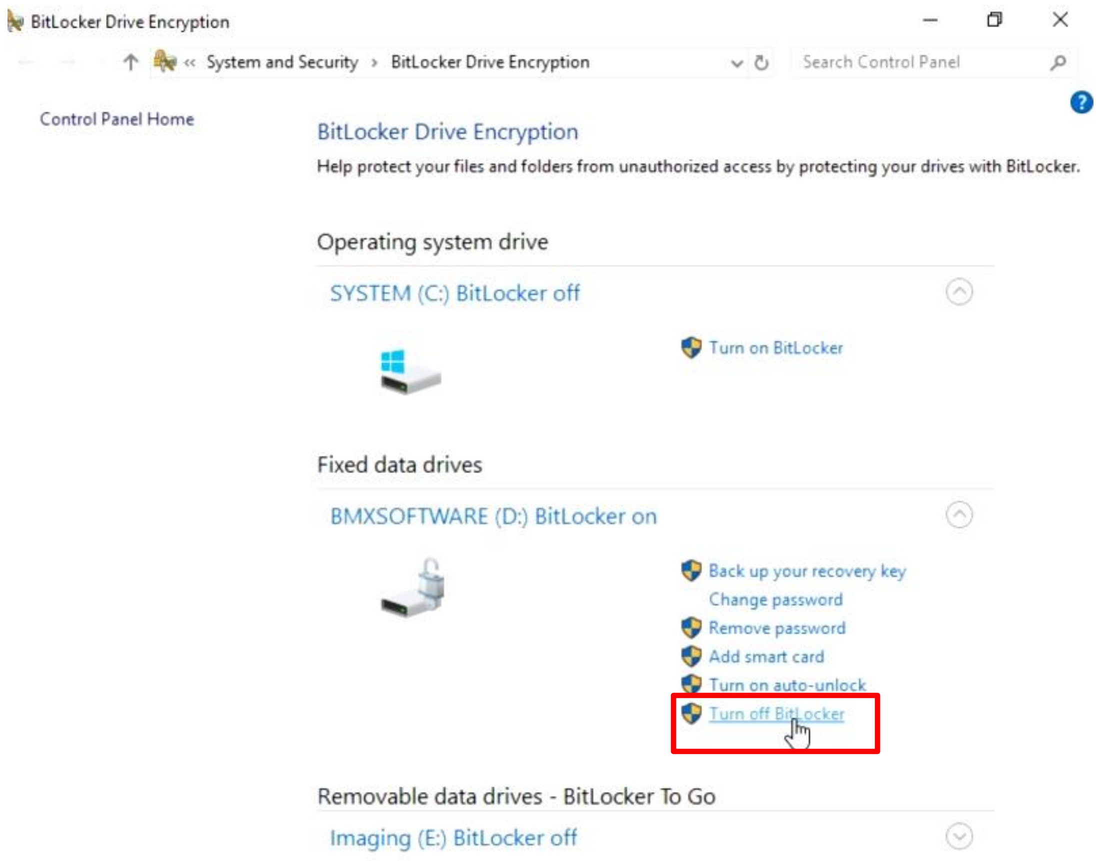
BitLocker (D:)

Enter password to unlock this drive.

BitLocker Drive Encryption
« System and Security › BitLocker Drive Encr
Control Panel Home
BitLocker Drive Encrypt
Help protect your files and fol
Operating system drive
SYSTEM (C:) BitLocker
Fixed data drives
D: BitLocker on (Locked)
Unlock drive
#1
#2
More options
Unlock
#3
Removable data drives - BitLocker To Go
Insert a removable USB flash drive to use BitLocker To Go.

Figure 30

6. Select **Turn off BitLocker** under the D: Drive Menu (*Figure* 31).



BitLocker Drive Encryption

System and Security › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

SYSTEM (C:) BitLocker off

Turn on BitLocker

Fixed data drives

BMXSOFTWARE (D:) BitLocker on

Back up your recovery key

Change password

Remove password

Add smart card

Turn on auto-unlock

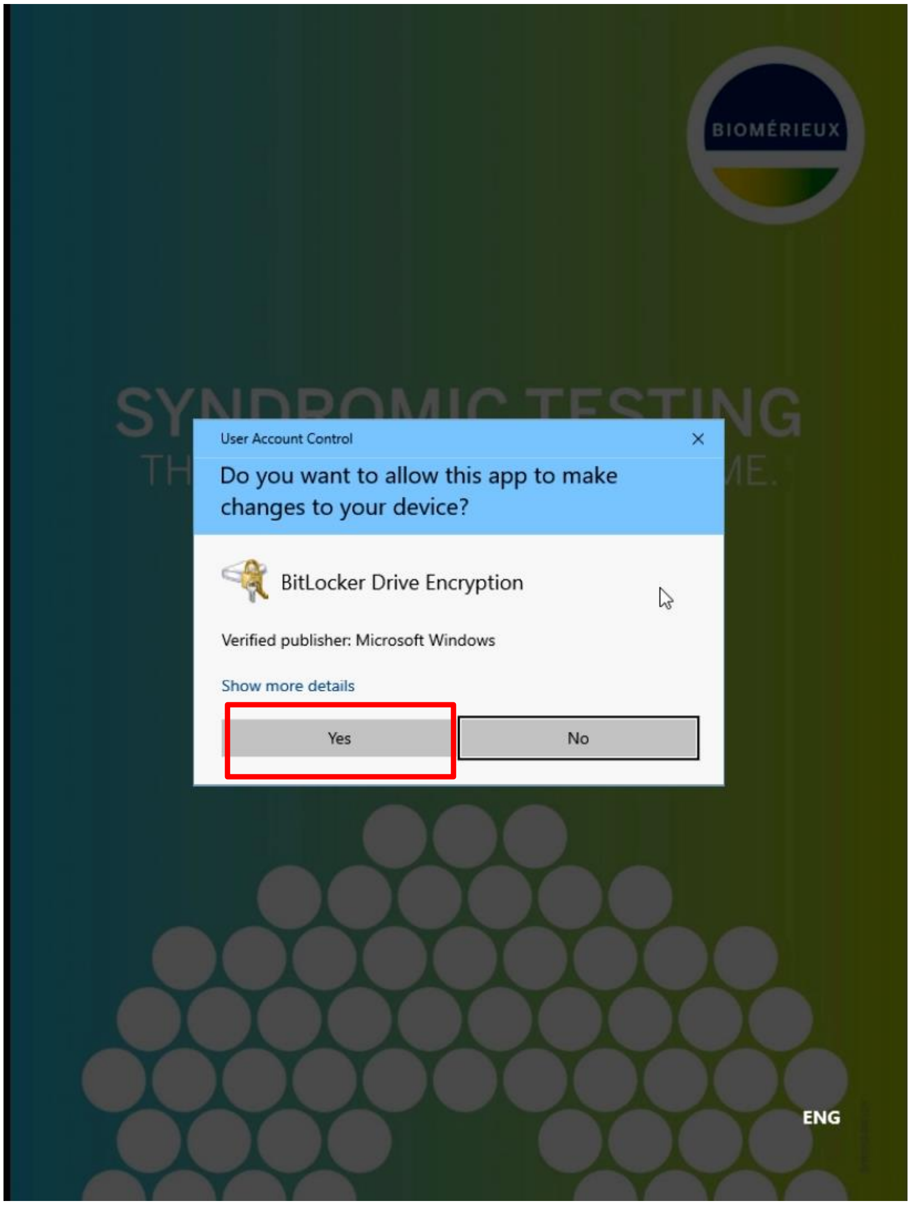
Turn off BitLocker

Removable data drives - BitLocker To Go

Imaging (E:) BitLocker off

Figure 31

7. Select **Yes** in the prompt “Do you want to allow this app to make changes to the device (*Figure* 32).



User Account Control

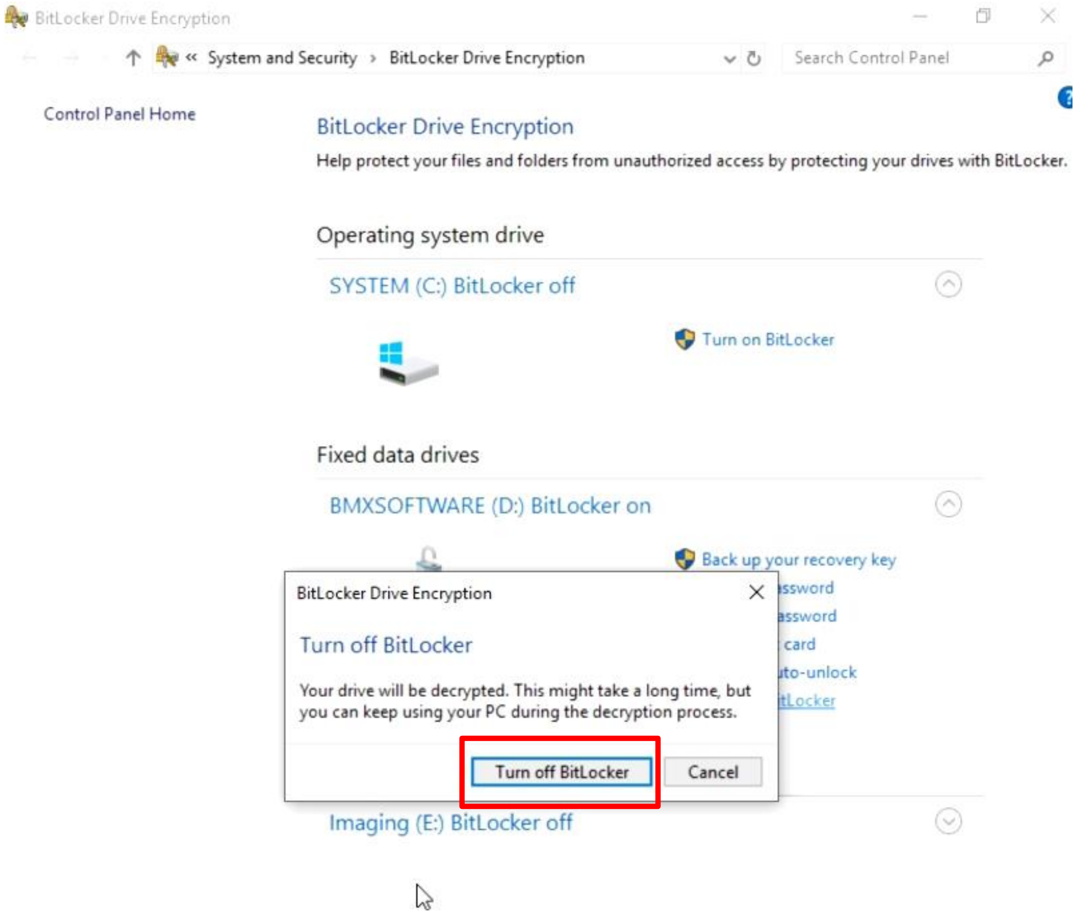
Do you want to allow this app to make changes to your device?

BitLocker Drive Encryption

Verified publisher: Microsoft Windows

Figure 32

8. Select **Turn off BitLocker** (*Figure* 33).


BitLocker Drive Encryption
System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption
Operating system drive
SYSTEM (C:) BitLocker off
Turn on BitLocker
Fixed data drives
BMXSOFTWARE (D:) BitLocker on
Back up your recovery key
assword
assword
card
ito-unlock
tLocker
BitLocker Drive Encryption
Turn off BitLocker
Turn off BitLocker
Cancel
Imaging (E:) BitLocker off

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

Figure 33

9. Once Decryption is complete, Restart the System to complete setup and return to the SPOTFIRE Software. Navigate to **Windows Start Menu → Power → Restart** (*Figure* 34).

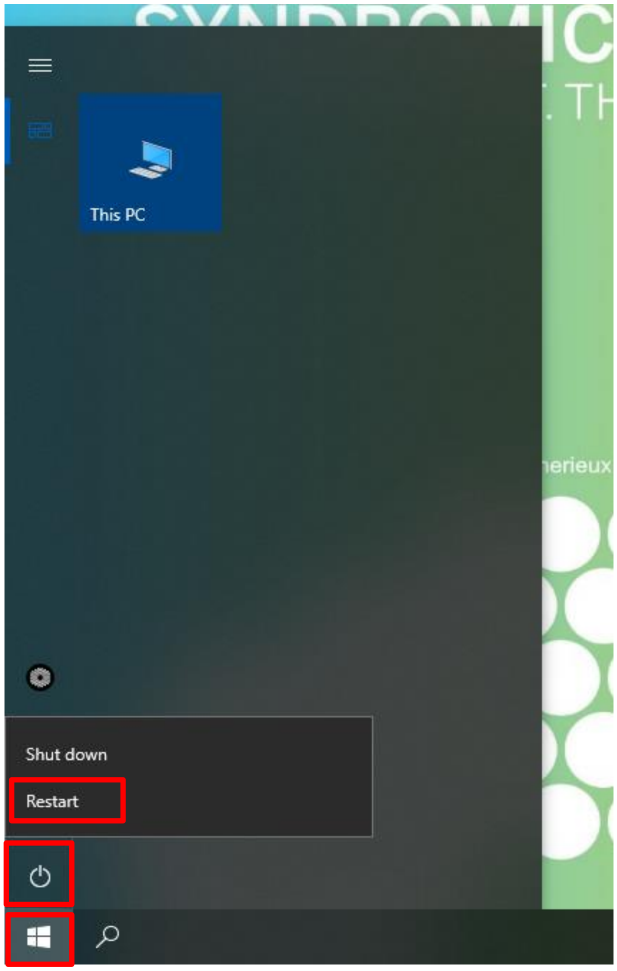


Figure 34

7. Technical Support Contact Information

bioMérieux is dedicated to providing the best customer support available. If you have any questions or concerns about this process, please contact the bioMérieux Technical Support team for assistance.

bioMérieux Technical Support
Email: biofiresupport@biomerieux.com
Phone: +1-801-736-6354, select Option 5

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

8. Frequently Asked Questions (FAQs)

Q: What happens if the customer loses their BitLocker Recovery Key?

> **A**: If the customer is still logged into the system, the customer can follow the Disabling BitLocker steps above and then re-enable BitLocker. If the user has lost the BitLocker Recovery Key and is locked out of the system, the customer needs to work with their IT department that has stored the systems recovery key.

Q: What happens if the customer loses their BitLocker Recovery Key and the system cannot be accessed by either the customer or the service center if it is returned for a service event?

> **A**: The hard drive cannot be accessed. The hard drive *may* need to be swapped for a hard drive field replaceable unit (FRU) if inaccessible. Data stored on the system *may* be lost if it was not backed up. Please contact the BIOFIRE Technical Support team for assistance.

9. Appendix

For more information regarding Microsoft BitLocker and configuration settings please refer to documentation on Microsoft's website:

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