BitLocker

BitLocker is a full disk encryption feature of Microsoft Windows which has been designed to protect data by providing encryption for entire drives. It helps secure data on lost or stolen devices, ensuring that unauthorized users cannot access the encrypted data.

Requirements

TPM(Trusted Platform Module) or USB drive: This is a hardware feature that stores encryption keys. A TPM version 1.2 or later is recommended. Alternative to TPM is USB drive. In this task, BitLocker encryption process is to be demonstrated using USB drive.

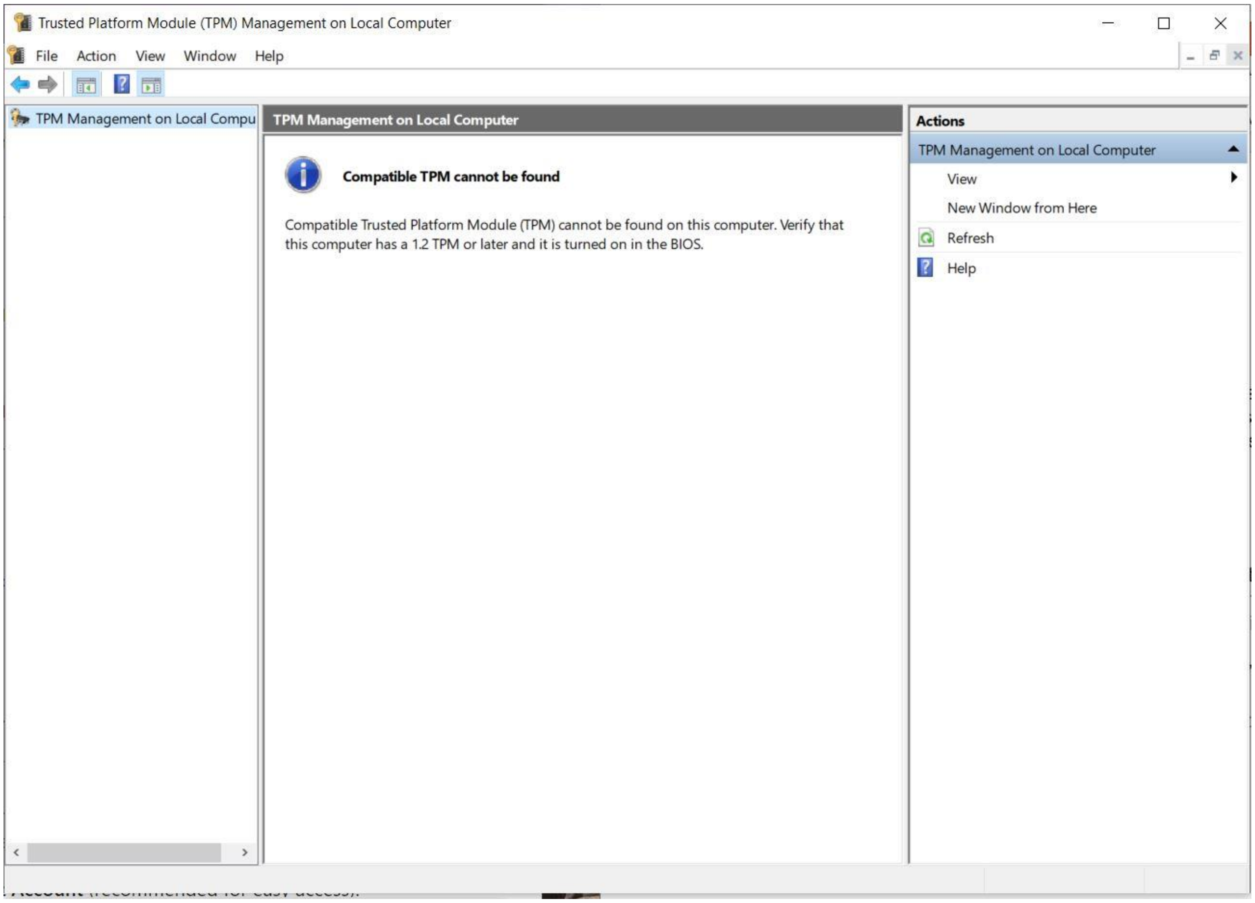
Windows Version: This feature is available only in Windows Professional, Enterprise and Education editions.

BIOS/UEFI Setting: TPM is required to be enabled.

Administrative Rights: Administrative privileges are required to enable BitLocker.

Steps to Encrypt and Decrypt Hard Drive with BitLocker

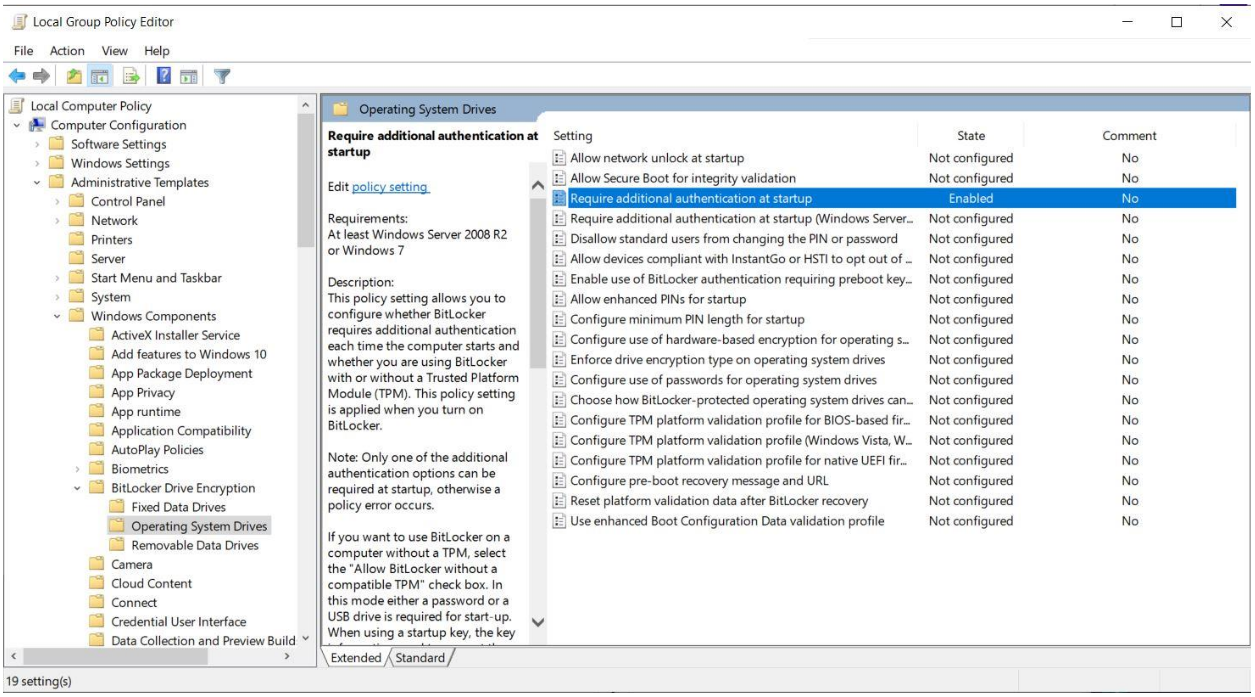
1. **Check for TPM Availability:** To open TPM Management Console, Windows + R pressed and then typed tpm.msc


Trusted Platform Module (TPM) Management on Local Computer
File
Action
View
Window
Help
TPM Management on Local Compu
TPM Management on Local Computer
Actions
TPM Management on Local Computer
View
New Window from Here
Refresh
Help

Compatible TPM cannot be found

Compatible Trusted Platform Module (TPM) cannot be found on this computer. Verify that this computer has a 1.2 TPM or later and it is turned on in the BIOS.

2. **Open Group Policy Editor:** Windows + R pressed and then typed gpedit.msc



Require additional authentication at startup

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

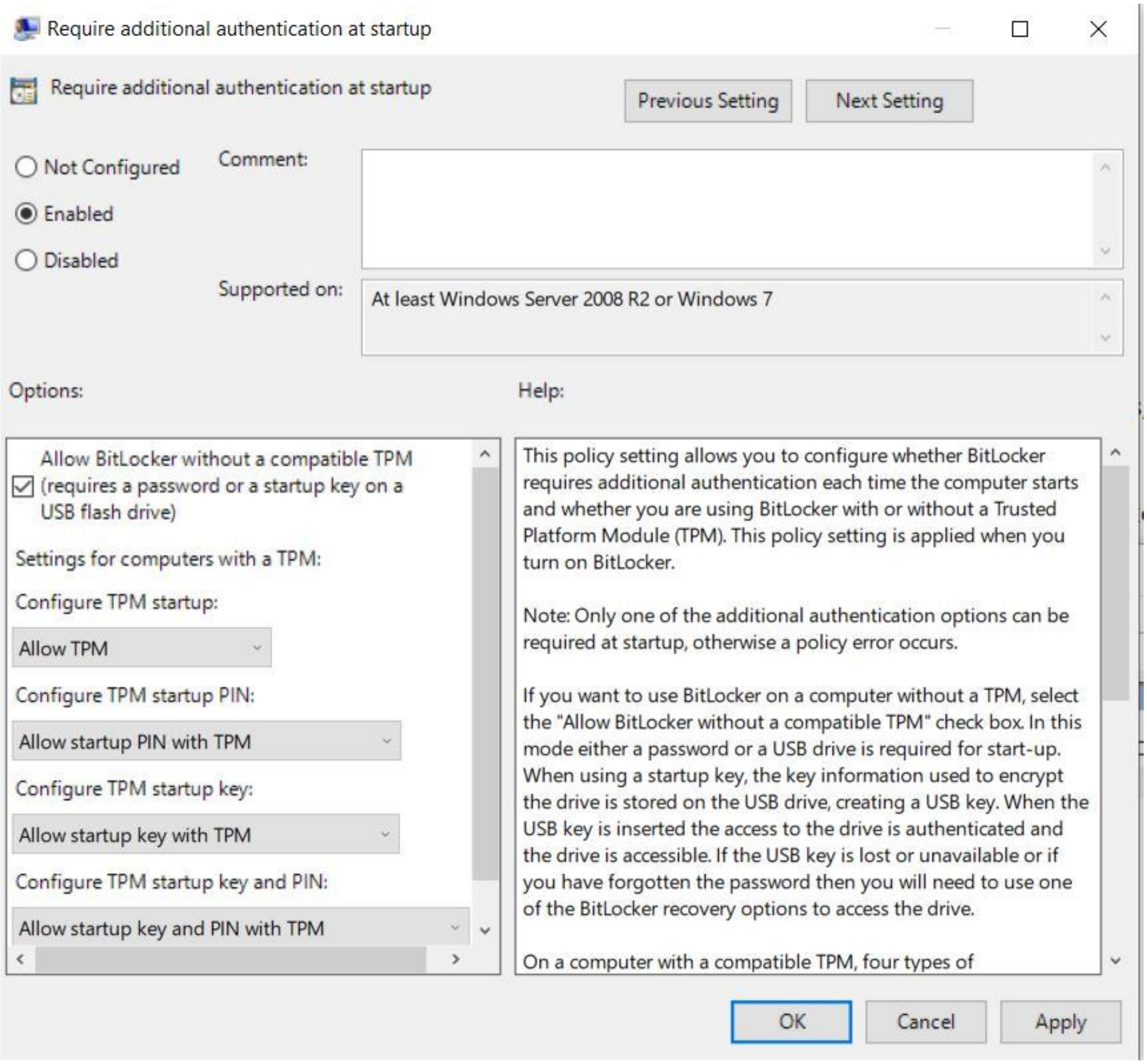
Description:
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key

Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Enabled	No
Require additional authentication at startup (Windows Server...	Not configured	No
Disallow standard users from changing the PIN or password	Not configured	No
Allow devices compliant with InstantGo or HSTI to opt out of ...	Not configured	No
Enable use of BitLocker authentication requiring preboot key...	Not configured	No
Allow enhanced PINs for startup	Not configured	No
Configure minimum PIN length for startup	Not configured	No
Configure use of hardware-based encryption for operating s...	Not configured	No
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives can...	Not configured	No
Configure TPM platform validation profile for BIOS-based fir...	Not configured	No
Configure TPM platform validation profile (Windows Vista, W...	Not configured	No
Configure TPM platform validation profile for native UEFI fir...	Not configured	No
Configure pre-boot recovery message and URL	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

3. **Configure Group Policy:** Double-clicked the Require additional authentication at startup policy. In the dialog that appears, selected Enabled. Checked the box for Allow BitLocker without a compatible TPM. Clicked Apply, then OK. Computer has been restarted to take the change in effect.



Require additional authentication at startup

Require additional authentication at startup

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

☑ Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup: Allow TPM

Configure TPM startup PIN: Allow startup PIN with TPM

Configure TPM startup key: Allow startup key with TPM

Configure TPM startup key and PIN: Allow startup key and PIN with TPM

Help:

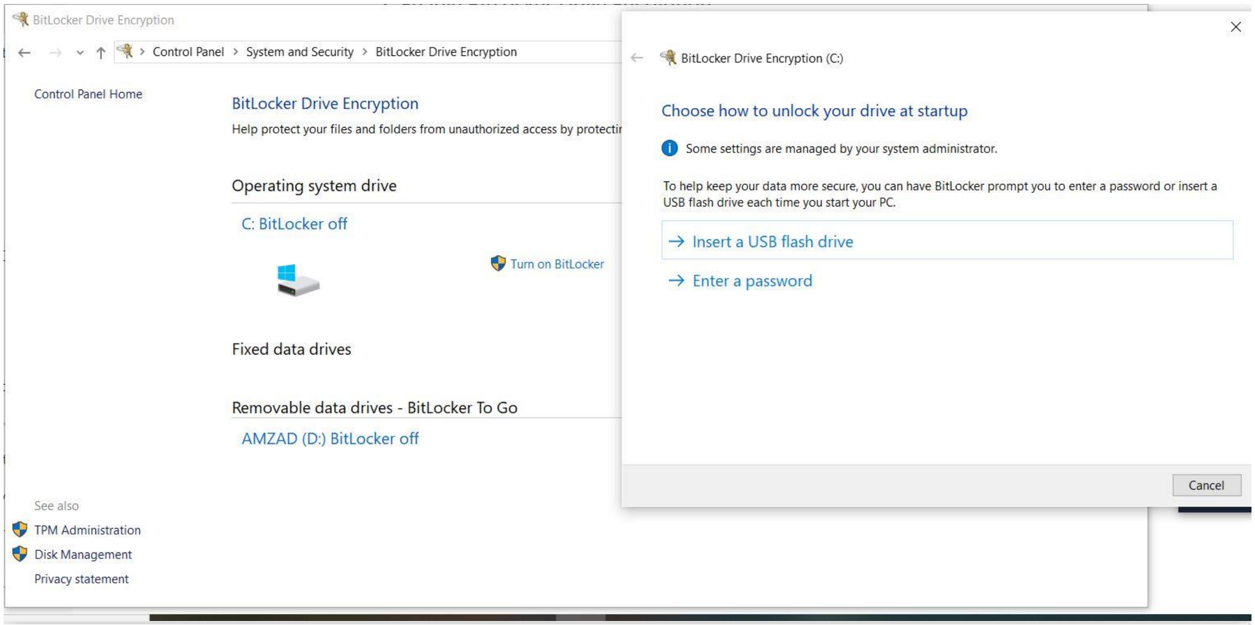
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of

4. **Enable BitLocker Drive Encryption:** Navigated to Control Panel > System and Security > BitLocker Drive Encryption. Following steps are demonstrated in the screencaps below.



BitLocker Drive Encryption

Control Panel > System and Security > BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protectir

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

AMZAD (D:) BitLocker off

See also

TPM Administration

Disk Management

Privacy statement

BitLocker Drive Encryption (C:)

Choose how to unlock your drive at startup

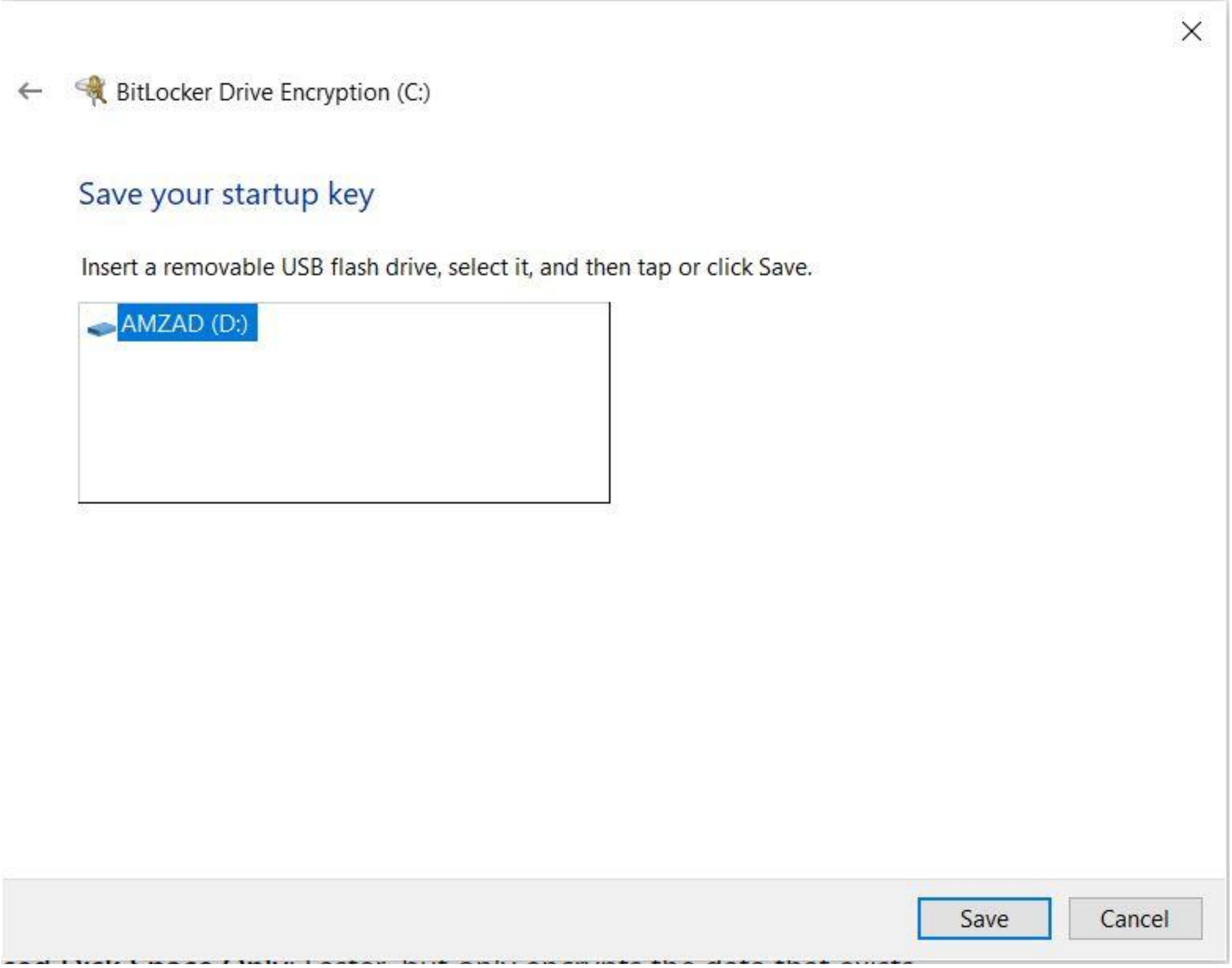
Some settings are managed by your system administrator.

To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.

→ Insert a USB flash drive

→ Enter a password

Cancel



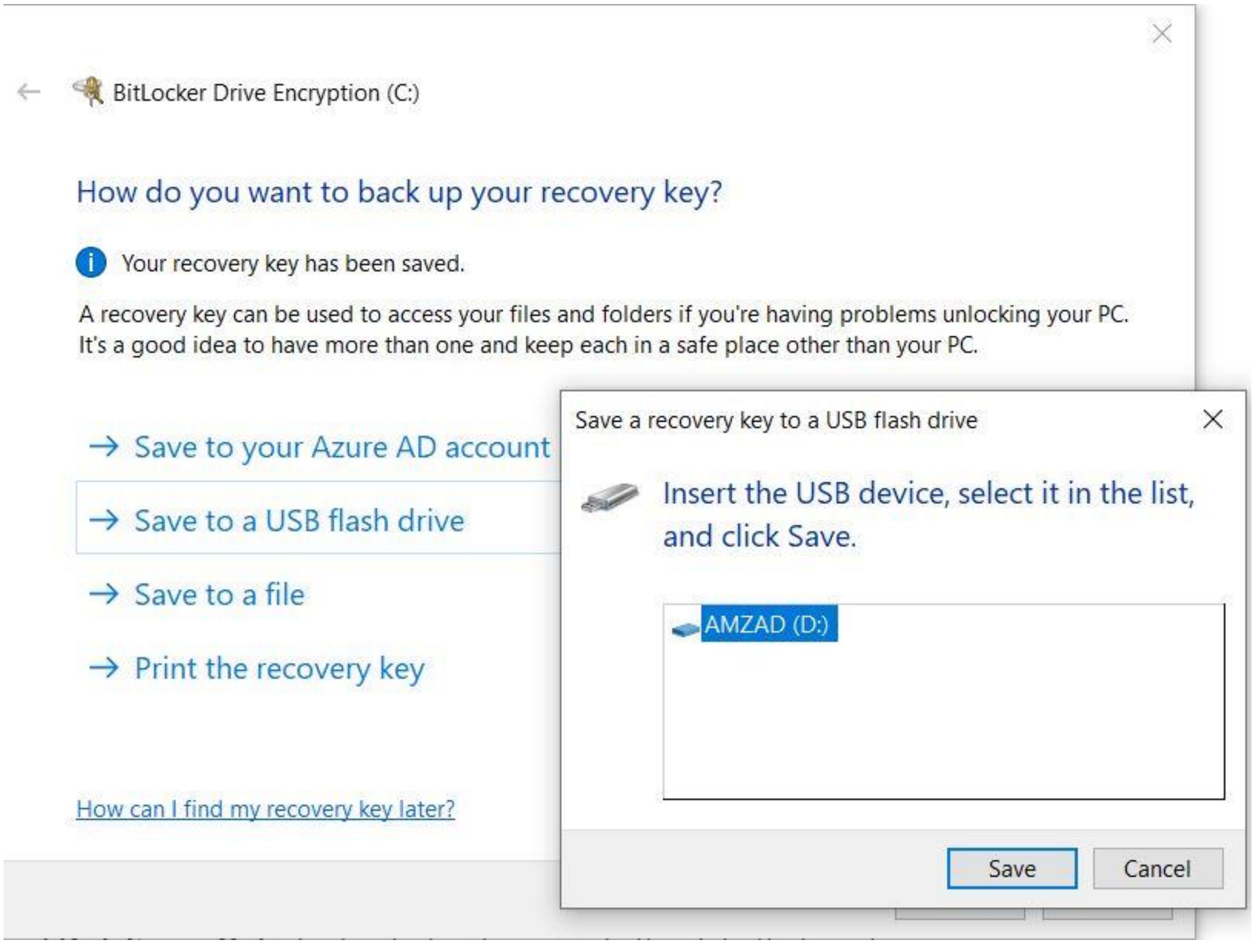
BitLocker Drive Encryption (C:)

Save your startup key

Insert a removable USB flash drive, select it, and then tap or click Save.

AMZAD (D:)

Save   Cancel



BitLocker Drive Encryption (C:)

How do you want to back up your recovery key?

Your recovery key has been saved.

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 Azure AD account

→ Save to a USB flash drive

→ Save to a file

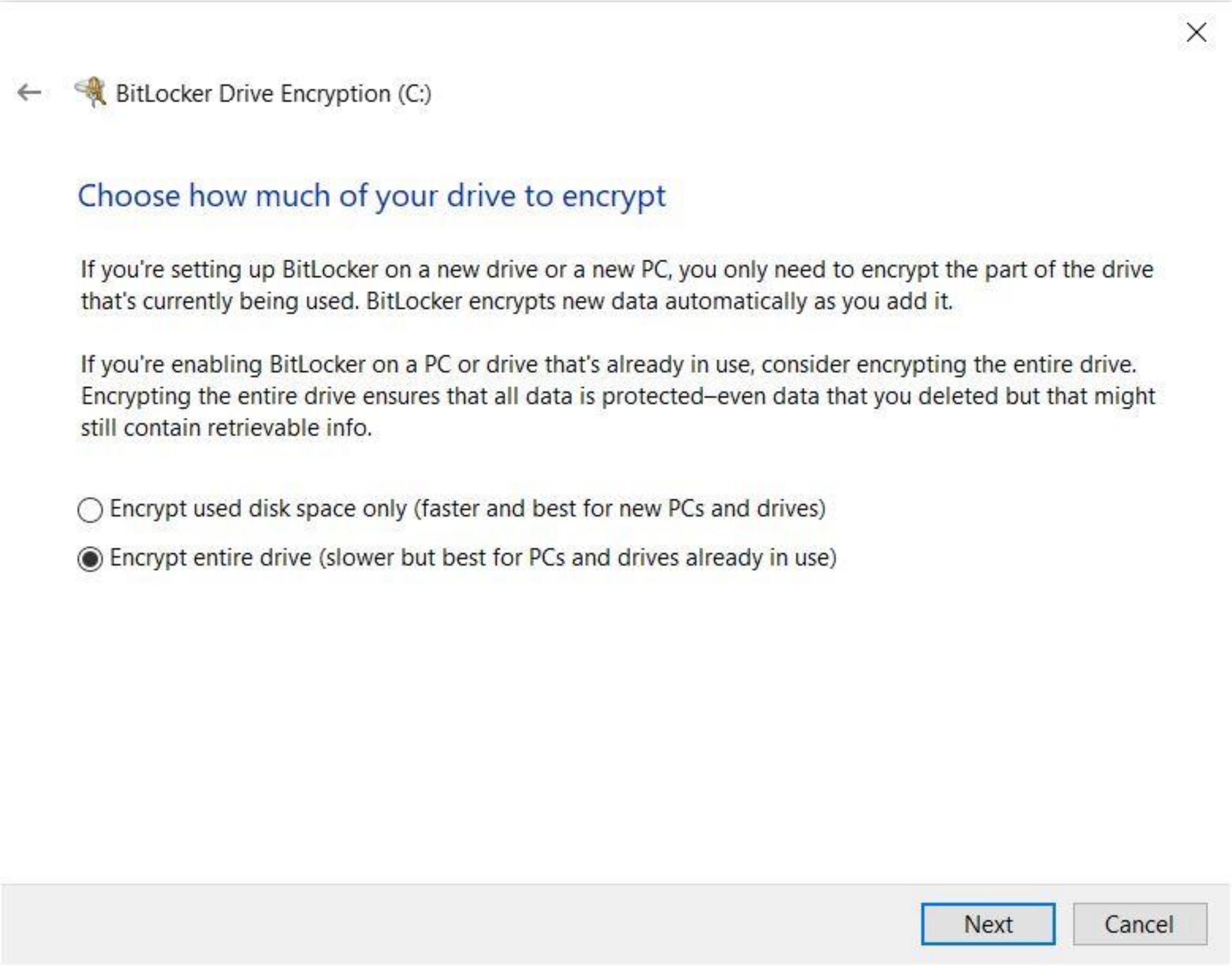
→ Print the recovery key

How can I find my recovery key later?

Save a recovery key to a USB flash drive

Insert the USB device, select it in the list, and click Save.

AMZAD (D:)



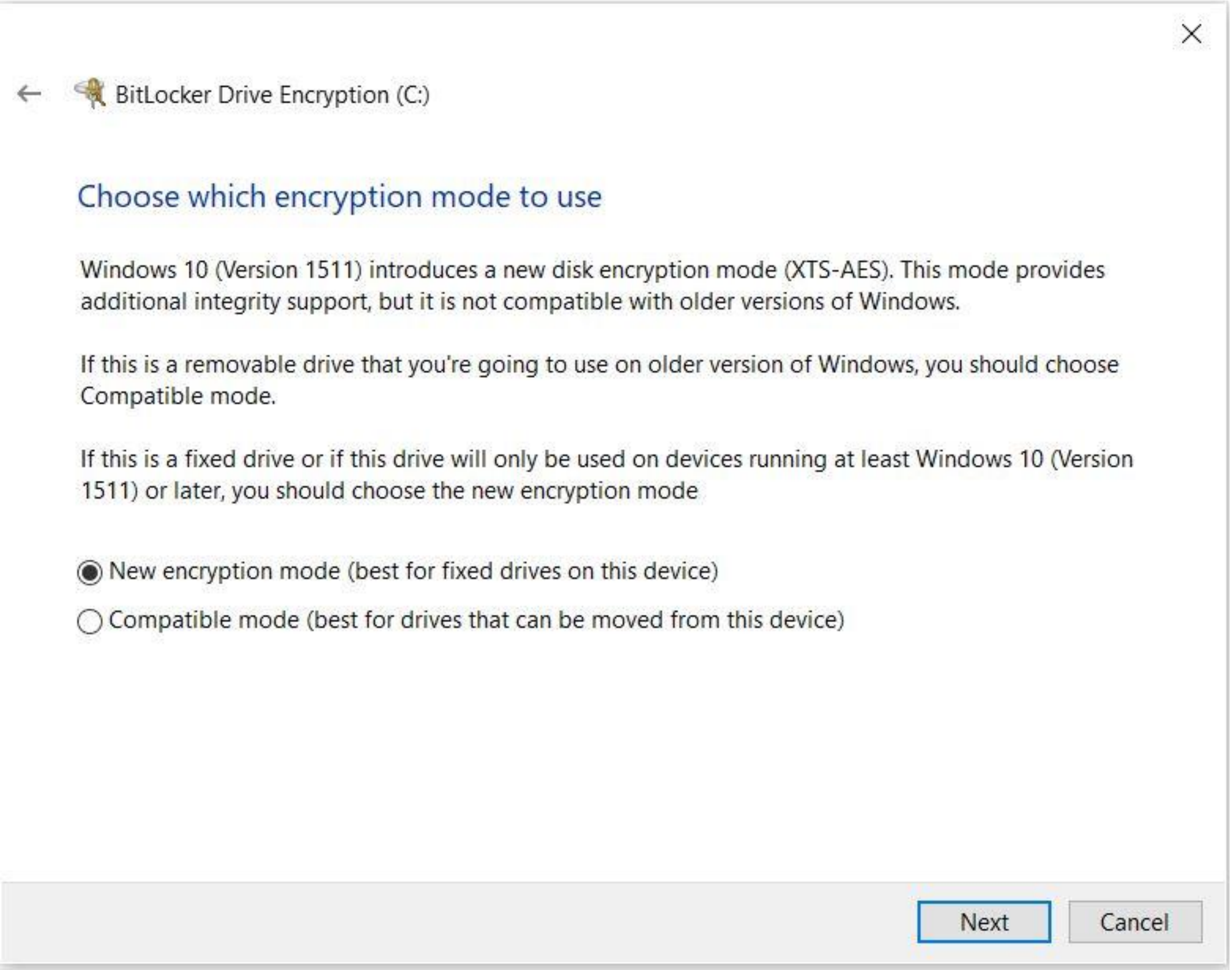
Choose how much of your drive to encrypt

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)



Choose which encryption mode to use

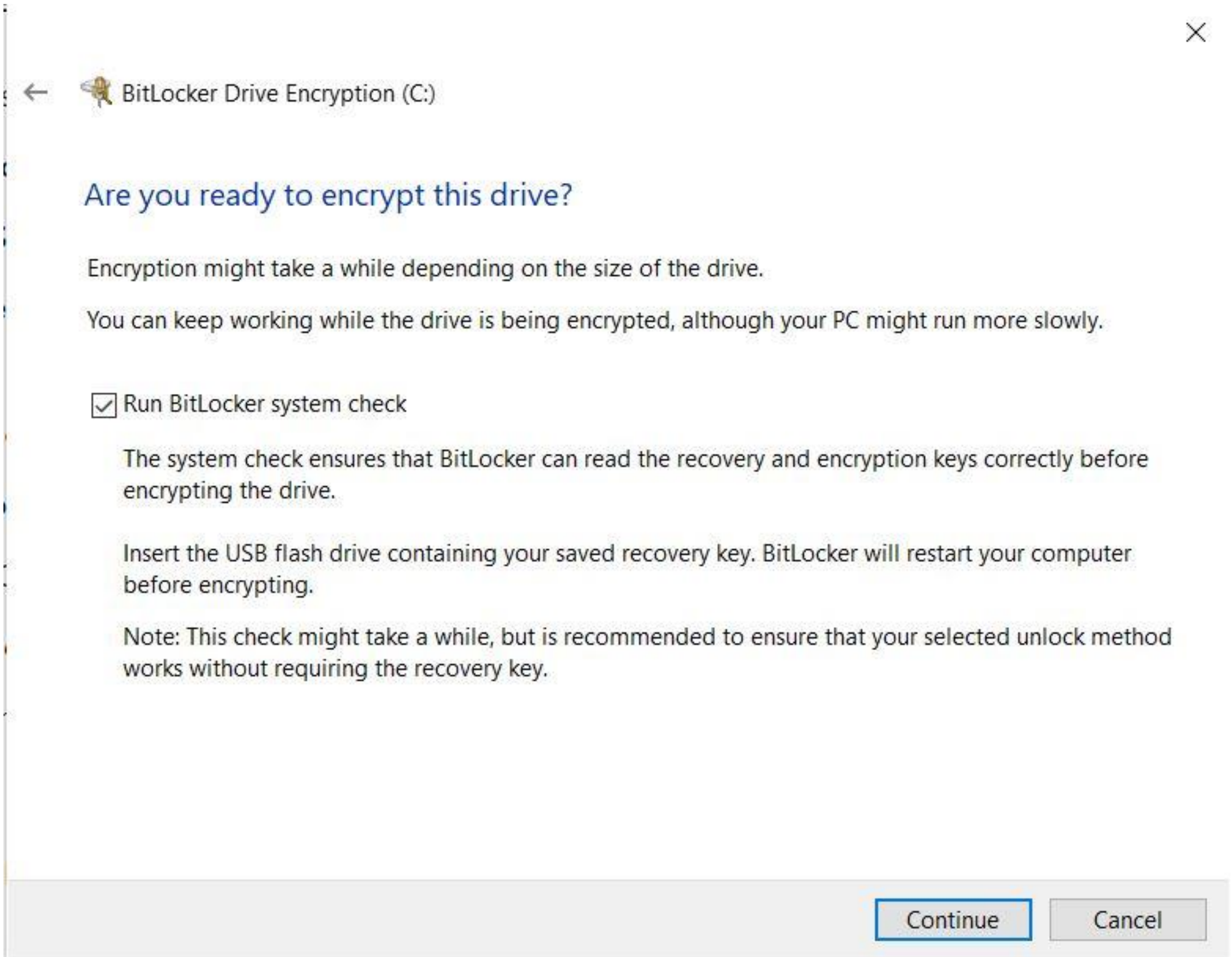
Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

● New encryption mode (best for fixed drives on this device)

○ Compatible mode (best for drives that can be moved from this device)



BitLocker Drive Encryption (C:)

Are you ready to encrypt this drive?

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

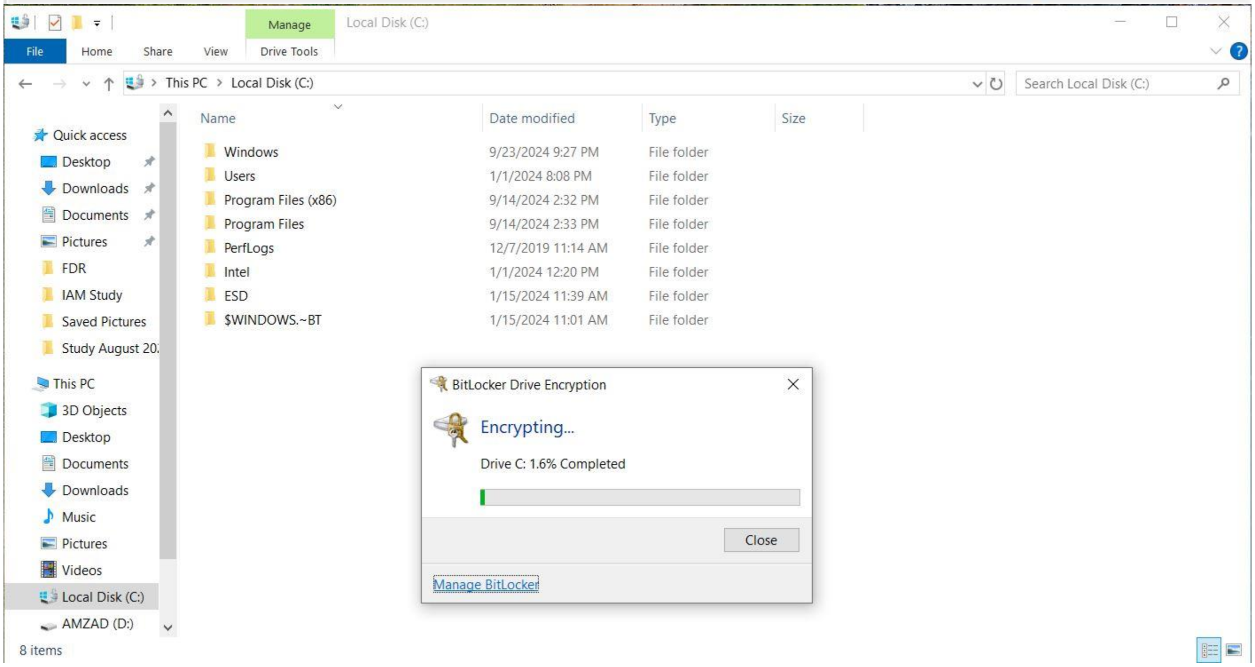
You can keep working while the drive is being encrypted, although your PC might run more slowly.

☑ Run BitLocker system check

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

Insert the USB flash drive containing your saved recovery key. 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.

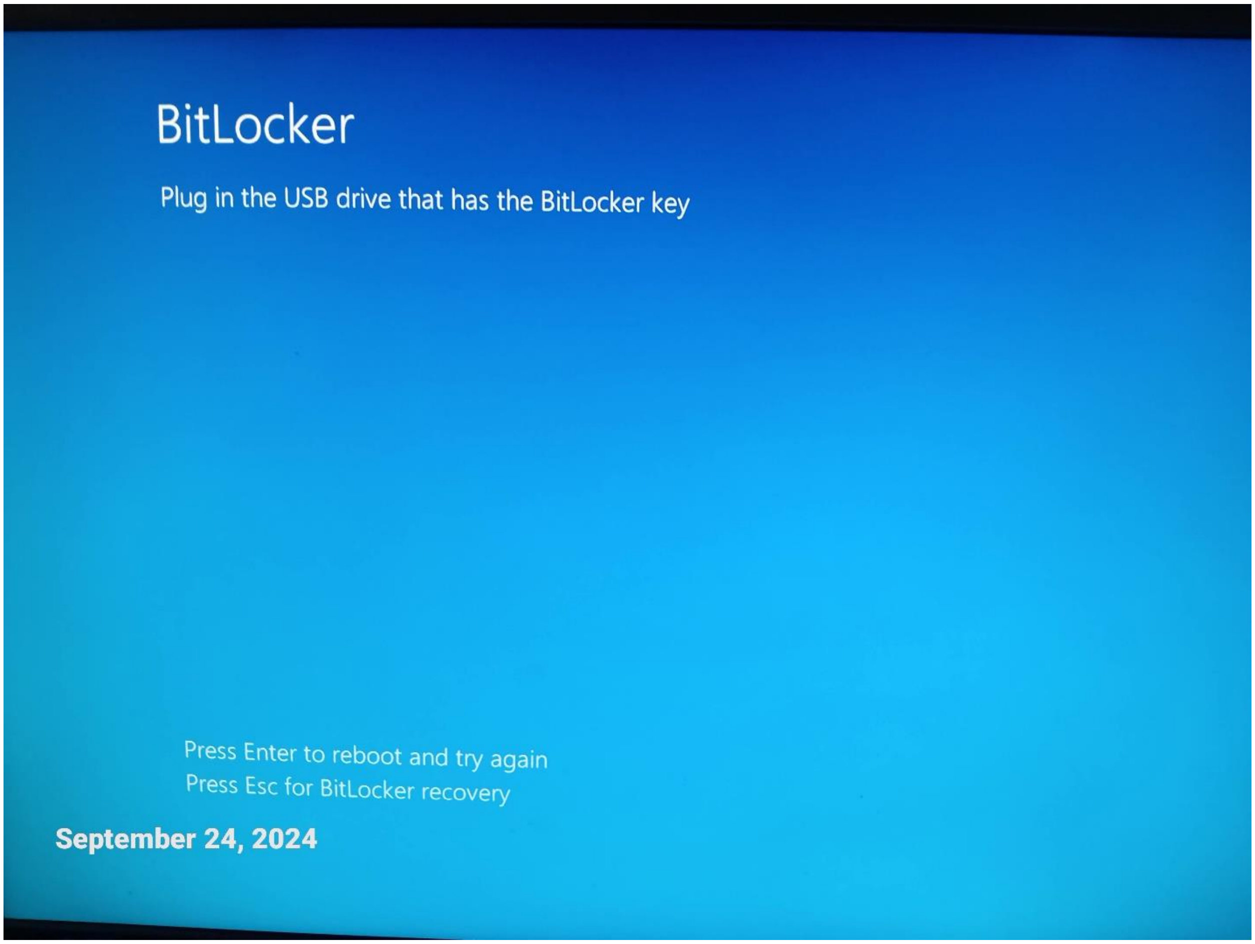


Name	Date modified	Type	Size
Windows	9/23/2024 9:27 PM	File folder	
Users	1/1/2024 8:08 PM	File folder	
Program Files (x86)	9/14/2024 2:32 PM	File folder	
Program Files	9/14/2024 2:33 PM	File folder	
PerfLogs	12/7/2019 11:14 AM	File folder	
Intel	1/1/2024 12:20 PM	File folder	
ESD	1/15/2024 11:39 AM	File folder	
$WINDOWS.~BT	1/15/2024 11:01 AM	File folder	

BitLocker Drive Encryption

Encrypting...

Drive C: 1.6% Completed



BitLocker

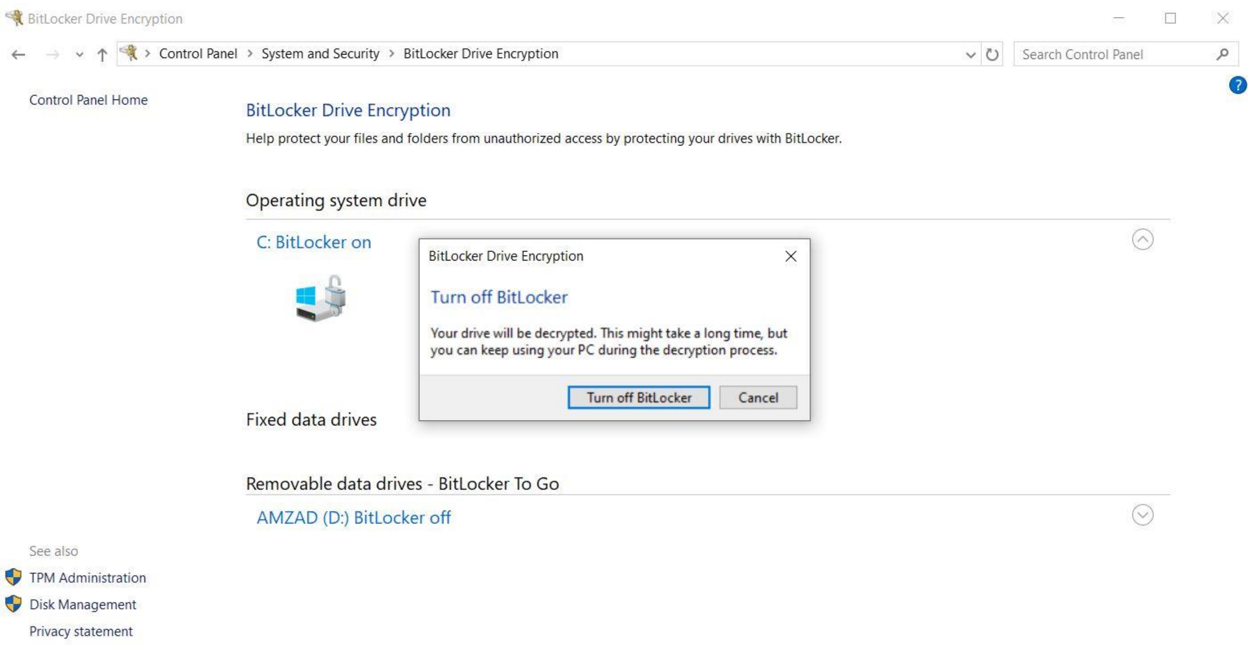
Plug in the USB drive that has the BitLocker key

Press Enter to reboot and try again

Press Esc for BitLocker recovery

September 24, 2024

5. **Disable BitLocker Drive Encryption:** Navigated to Control Panel > System and Security > BitLocker Drive Encryption. Following steps are demonstrated in the screencaps below.


BitLocker Drive Encryption
Control Panel > 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

C: BitLocker on

BitLocker Drive Encryption

Turn off BitLocker

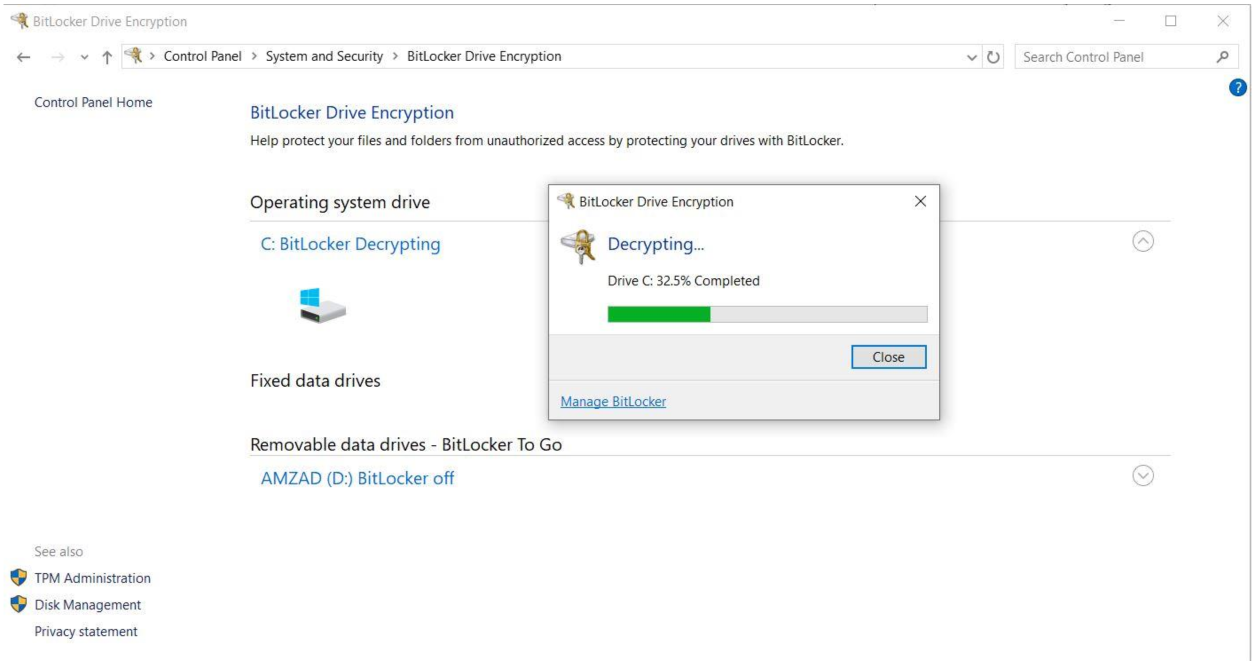
Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

Turn off BitLocker
Cancel

Fixed data drives

Removable data drives - BitLocker To Go

AMZAD (D:) BitLocker off


BitLocker Drive Encryption
Control Panel > 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

C: BitLocker Decrypting

BitLocker Drive Encryption

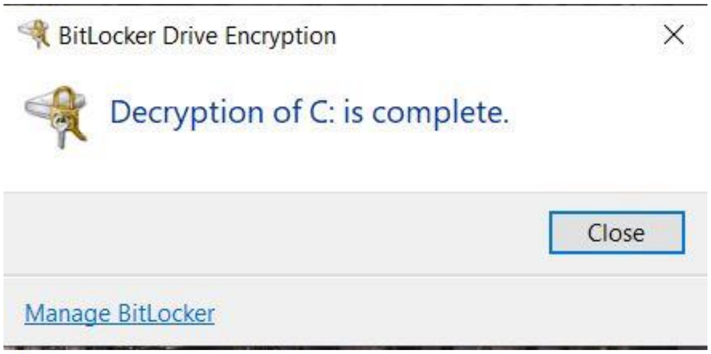
Decrypting...

Drive C: 32.5% Completed

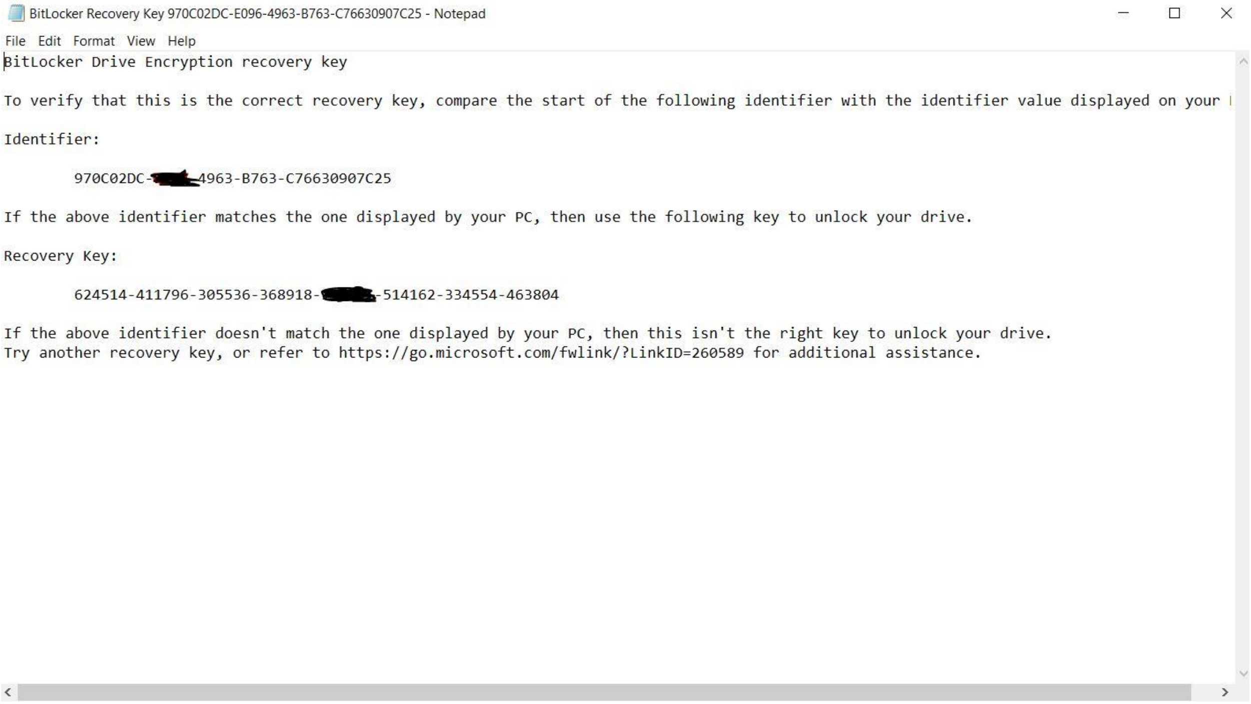
Fixed data drives

Removable data drives - BitLocker To Go

AMZAD (D:) BitLocker off



Decryption of C: is complete.

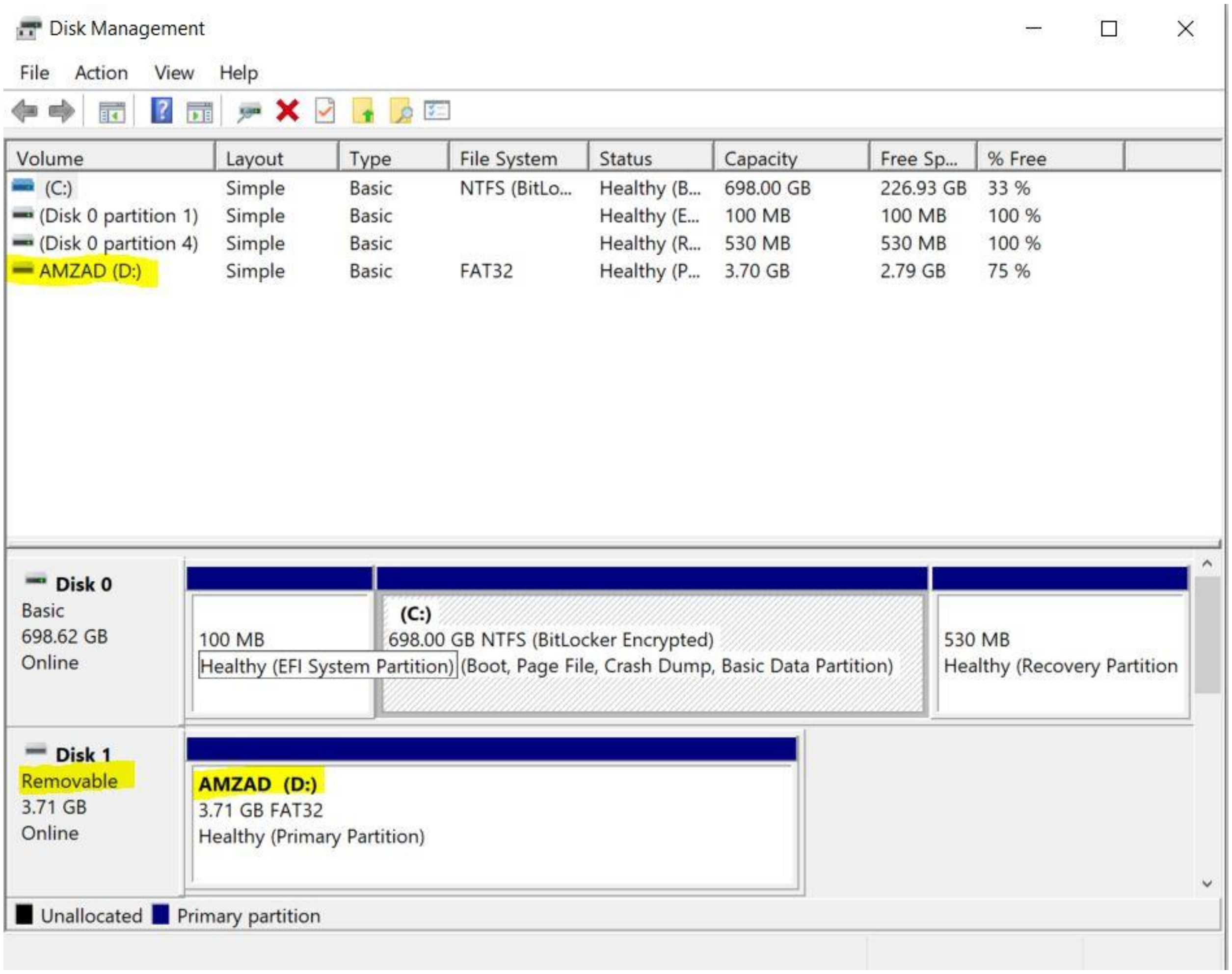

BitLocker Recovery Key 970C02DC-E096-4963-B763-C76630907C25 - Notepad
File Edit Format View Help

```
BitLocker Drive Encryption recovery key

To verify that this is the correct recovery key, compare the start of the following identifier with the identifier value displayed on your

Identifier:

        970C02DC-[redacted]4963-B763-C76630907C25

If the above identifier matches the one displayed by your PC, then use the following key to unlock your drive.

Recovery Key:

        624514-411796-305536-368918-[redacted]-514162-334554-463804

If the above identifier doesn't match the one displayed by your PC, then this isn't the right key to unlock your drive.
Try another recovery key, or refer to https://go.microsoft.com/fwlink/?LinkID=260589 for additional assistance.
```

Hiding a Flash Drive

To hide a flash drive-

- **Removed the Drive Letter**
- **Right-clicked the Start button > selected Disk Management..**
- **Right-clicked the drive and choosen Change Drive Letter and Paths.**
- **Clicked Remove to unassign its drive letter, making it invisible in File Explorer.**



Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS (BitLo...	Healthy (B...	698.00 GB	226.93 GB	33 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	530 MB	530 MB	100 %
AMZAD (D:)	Simple	Basic	FAT32	Healthy (P...	3.70 GB	2.79 GB	75 %

Disk 0
Basic
698.62 GB
Online

100 MB
Healthy (EFI System Partition)

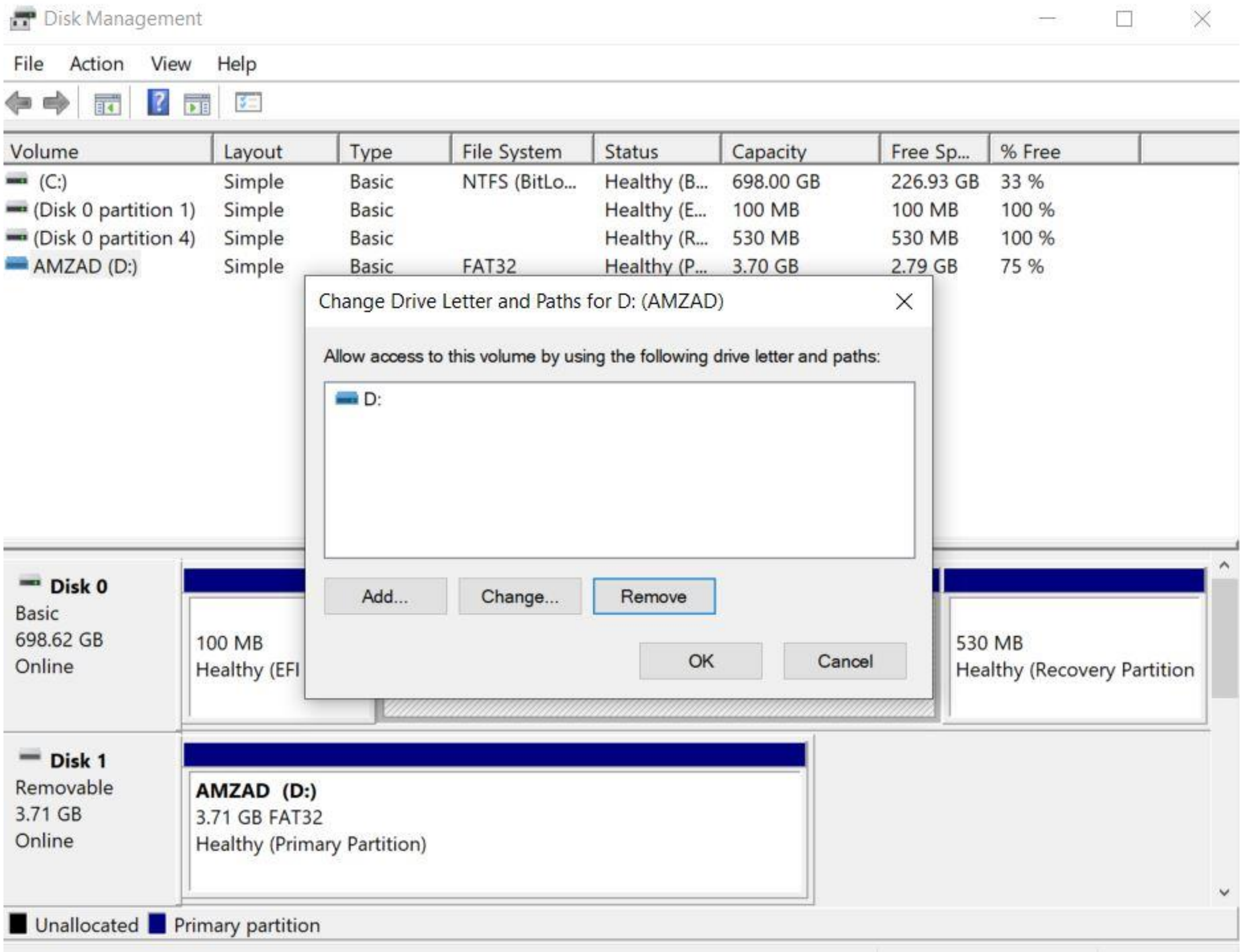
(C:)
698.00 GB NTFS (BitLocker Encrypted)
(Boot, Page File, Crash Dump, Basic Data Partition)

530 MB
Healthy (Recovery Partition

Disk 1
Removable
3.71 GB
Online

AMZAD (D:)
3.71 GB FAT32
Healthy (Primary Partition)

■ Unallocated ■ Primary partition



Disk Management

Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS (BitLo...	Healthy (B...	698.00 GB	226.93 GB	33 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	530 MB	530 MB	100 %
AMZAD (D:)	Simple	Basic	FAT32	Healthy (P...	3.70 GB	2.79 GB	75 %

Change Drive Letter and Paths for D: (AMZAD)

Allow access to this volume by using the following drive letter and paths:

D:

Disk 0
Basic
698.62 GB
Online

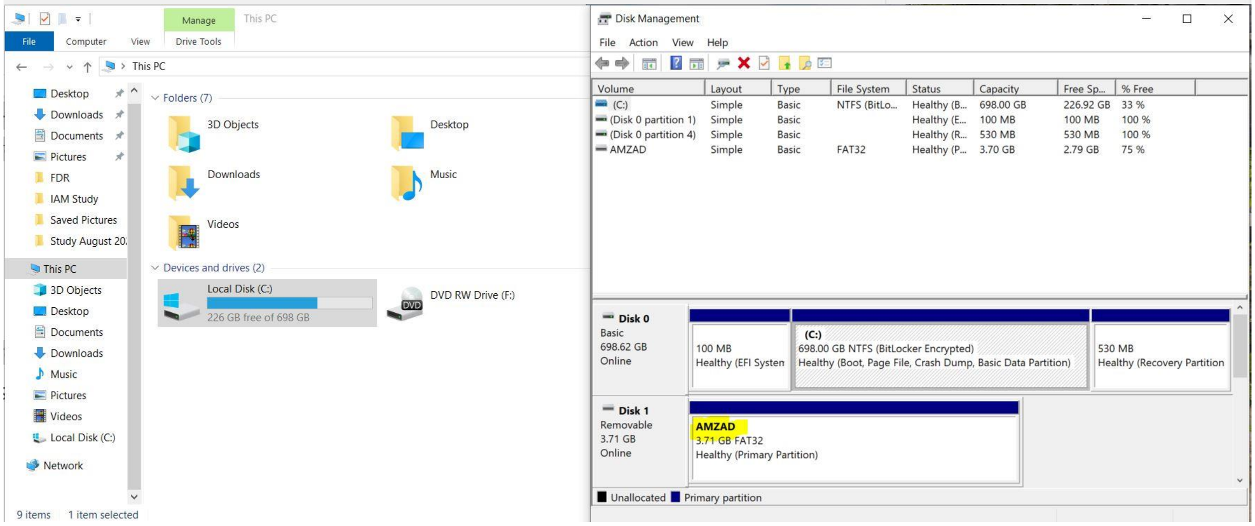
100 MB
Healthy (EFI

530 MB
Healthy (Recovery Partition

Disk 1
Removable
3.71 GB
Online

AMZAD (D:)
3.71 GB FAT32
Healthy (Primary Partition)

■ Unallocated ■ Primary partition



Local Disk (C:)
226 GB free of 698 GB

9 items 1 item selected

Disk Management

Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS (BitLo...	Healthy (B...	698.00 GB	226.92 GB	33 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	530 MB	530 MB	100 %
AMZAD	Simple	Basic	FAT32	Healthy (P...	3.70 GB	2.79 GB	75 %

Disk 0
Basic
698.62 GB
Online

100 MB
Healthy (EFI Systen

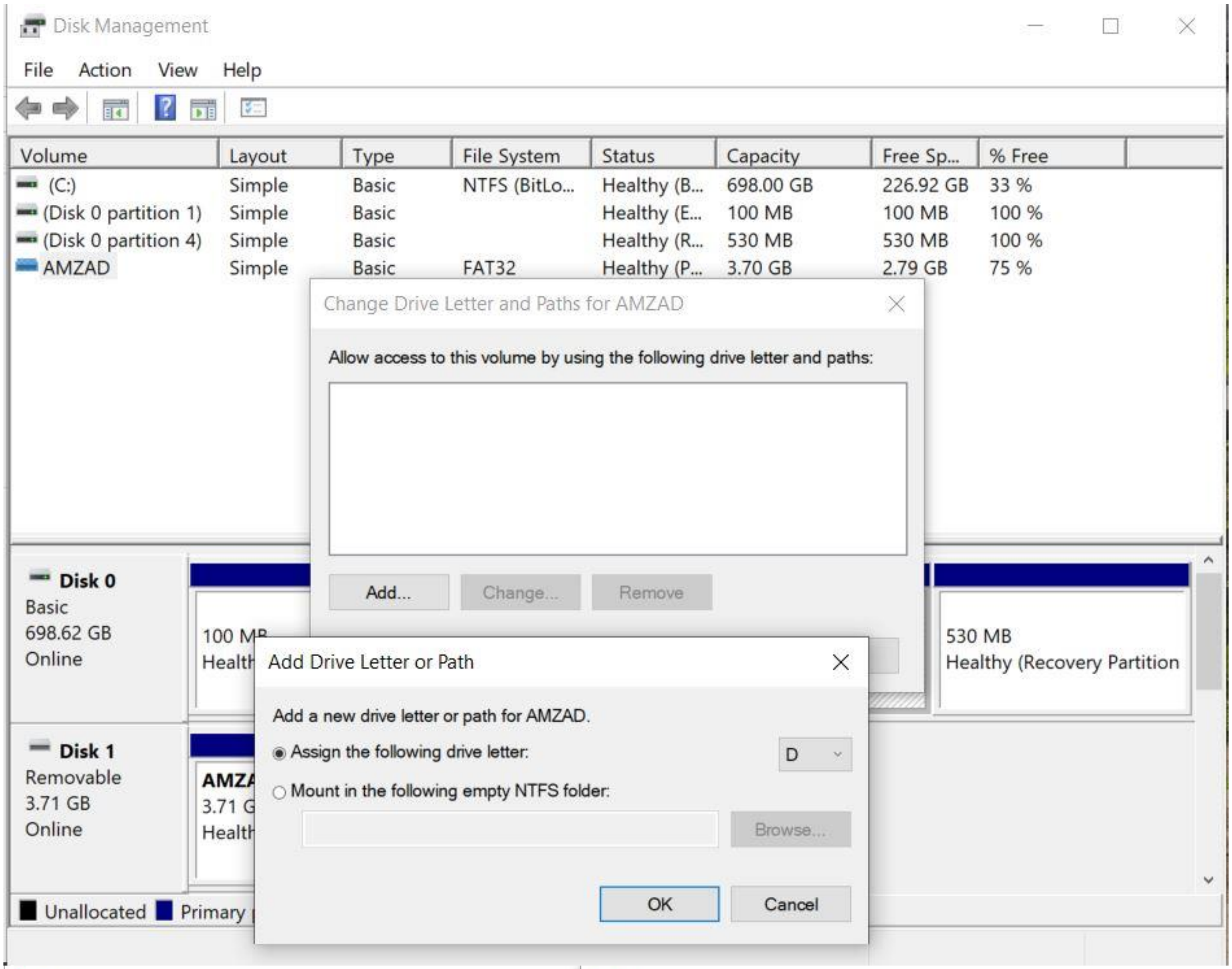
(C:)
698.00 GB NTFS (BitLocker Encrypted)
Healthy (Boot, Page File, Crash Dump, Basic Data Partition)

530 MB
Healthy (Recovery Partition

Disk 1
Removable
3.71 GB
Online

AMZAD
3.71 GB FAT32
Healthy (Primary Partition)

■ Unallocated ■ Primary partition



Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS (BitLo...	Healthy (B...	698.00 GB	226.92 GB	33 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	530 MB	530 MB	100 %
AMZAD	Simple	Basic	FAT32	Healthy (P...	3.70 GB	2.79 GB	75 %

Disk 0
Basic
698.62 GB
Online

100 MB
Health

530 MB
Healthy (Recovery Partition

Disk 1
Removable
3.71 GB
Online

AMZA
3.71 G
Health

■ Unallocated ■ Primary

Change Drive Letter and Paths for AMZAD

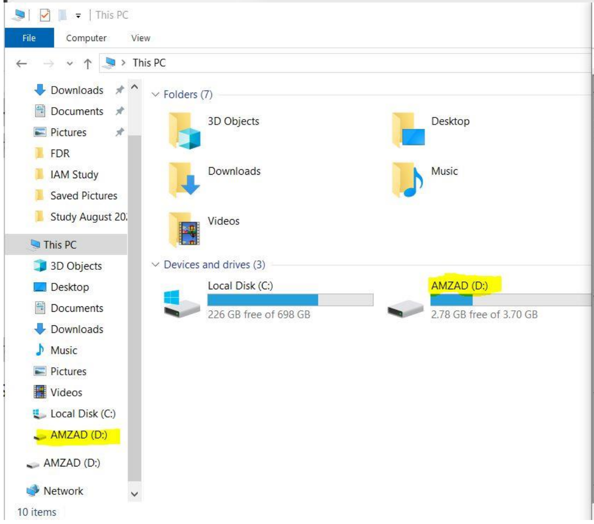
Allow access to this volume by using the following drive letter and paths:

Add Drive Letter or Path

Add a new drive letter or path for AMZAD.

● Assign the following drive letter: D

○ Mount in the following empty NTFS folder:



Folders (7)

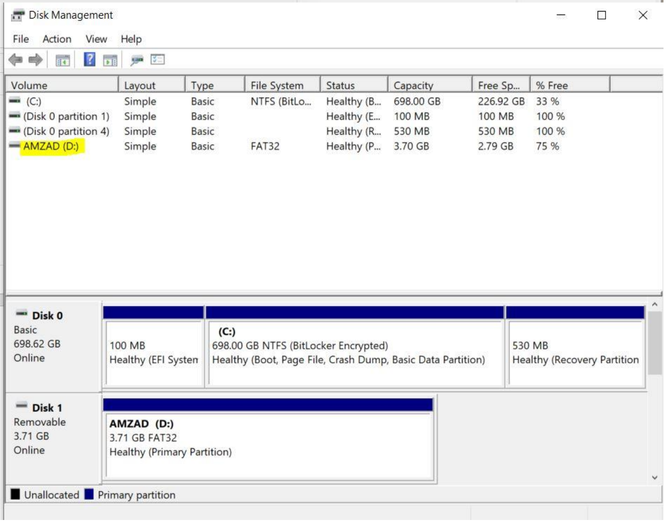
3D Objects
Desktop
Downloads
Music
Videos

Devices and drives (3)

Local Disk (C:)
226 GB free of 698 GB

AMZAD (D:)
2.78 GB free of 3.70 GB

10 items



Volume	Layout	Type	File System	Status	Capacity	Free Sp...	% Free
(C:)	Simple	Basic	NTFS (BitLo...	Healthy (B...	698.00 GB	226.92 GB	33 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	530 MB	530 MB	100 %
AMZAD (D:)	Simple	Basic	FAT32	Healthy (P...	3.70 GB	2.79 GB	75 %

Disk 0
Basic
698.62 GB
Online

100 MB
Healthy (EFI Systen

(C:)
698.00 GB NTFS (BitLocker Encrypted)
Healthy (Boot, Page File, Crash Dump, Basic Data Partition)

530 MB
Healthy (Recovery Partition

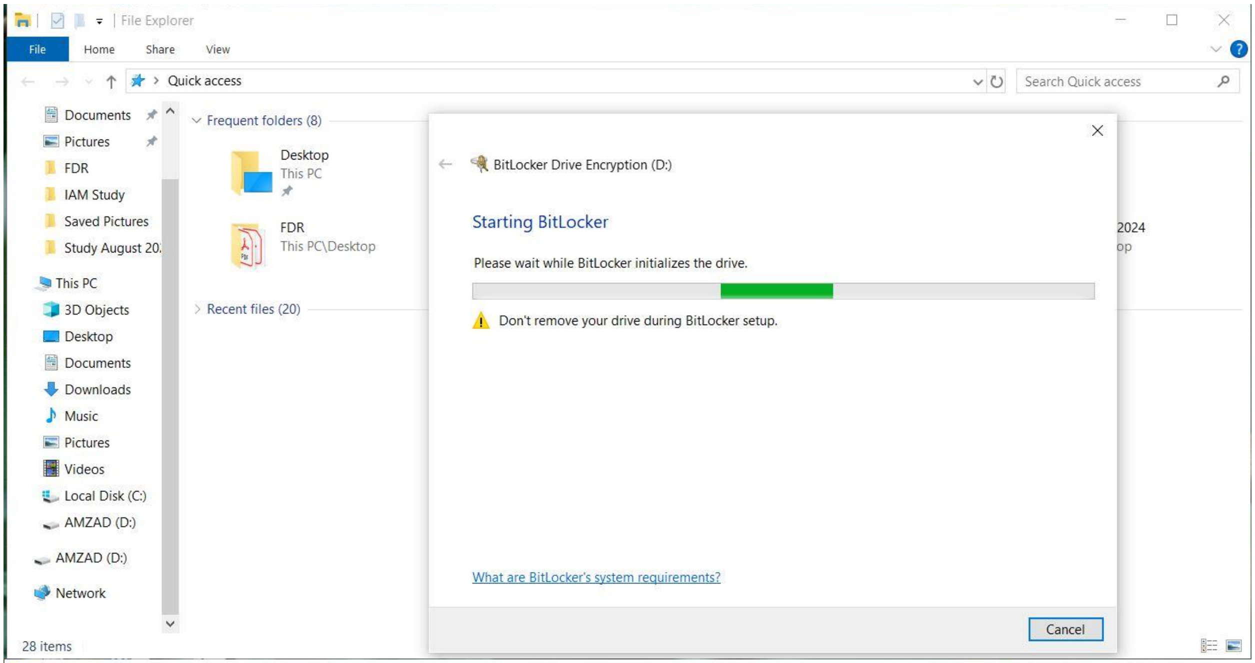
Disk 1
Removable
3.71 GB
Online

AMZAD (D:)
3.71 GB FAT32
Healthy (Primary Partition)

■ Unallocated ■ Primary partition

Steps to Encrypt and Decrypt Flash Drive with BitLocker

We follow the similar way to encrypt Flash Drive using BitLocker as demonstrated before. Here the screencaps are shown in sequence to follow the steps:



BitLocker Drive Encryption (D:)

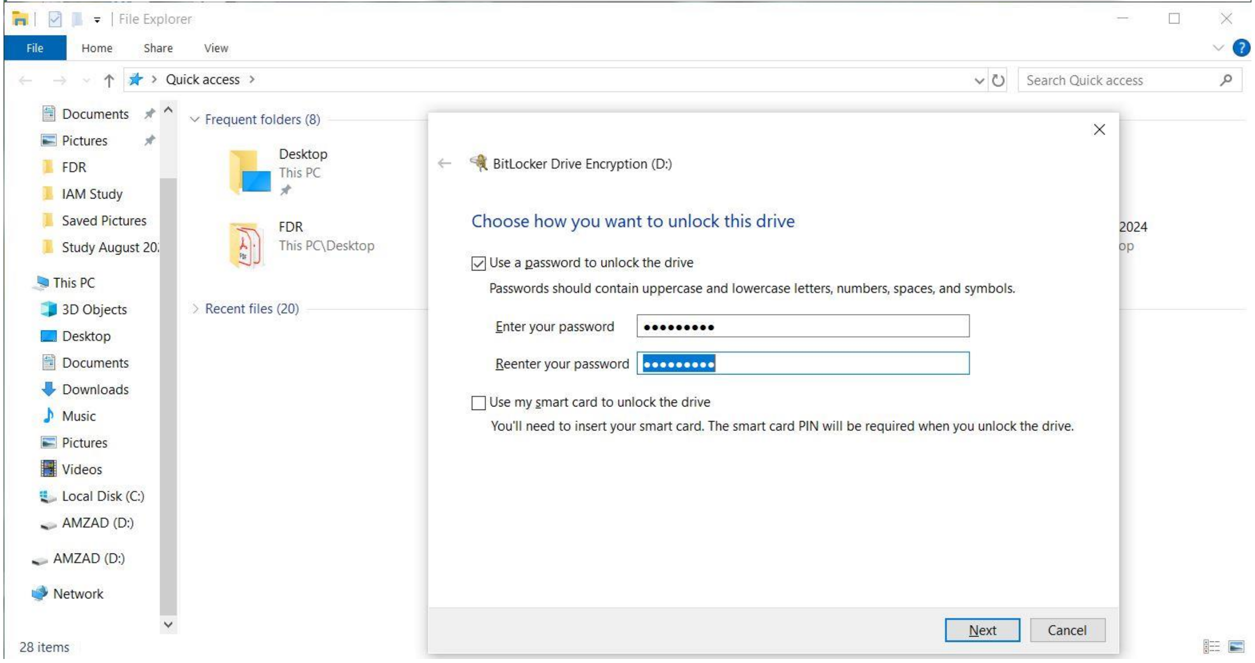
Starting BitLocker

Please wait while BitLocker initializes the drive.

⚠ Don't remove your drive during BitLocker setup.

What are BitLocker's system requirements?

Cancel



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.

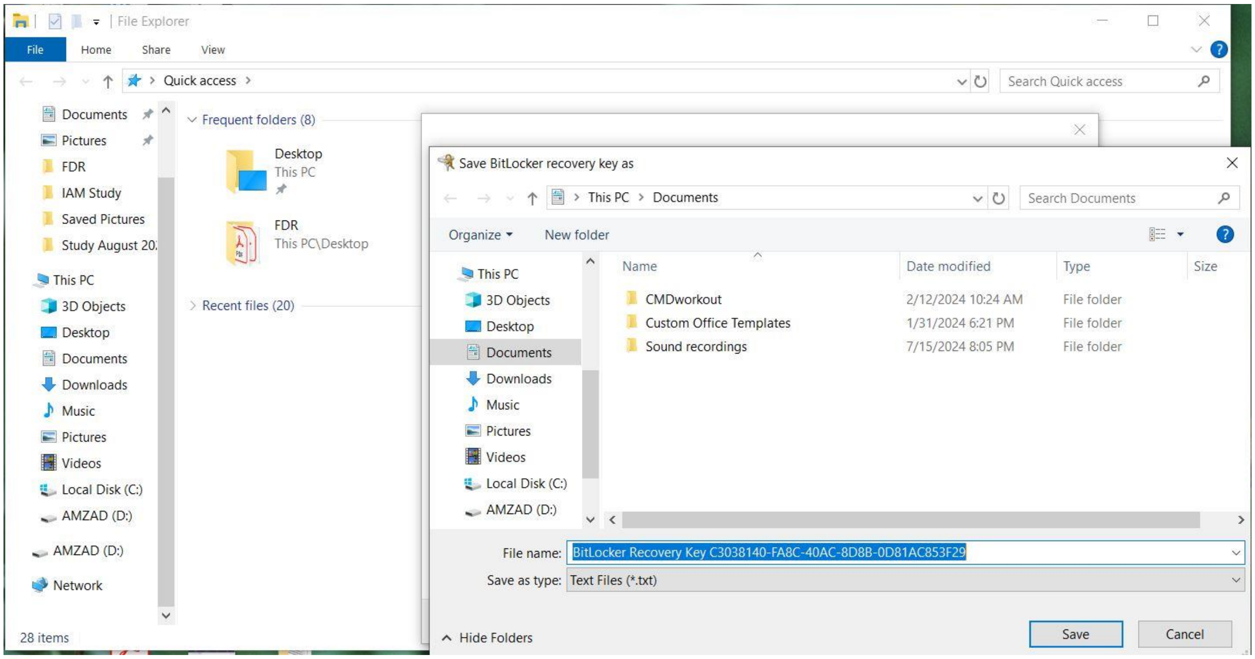
Enter your password ●●●●●●●●●

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.

Next Cancel



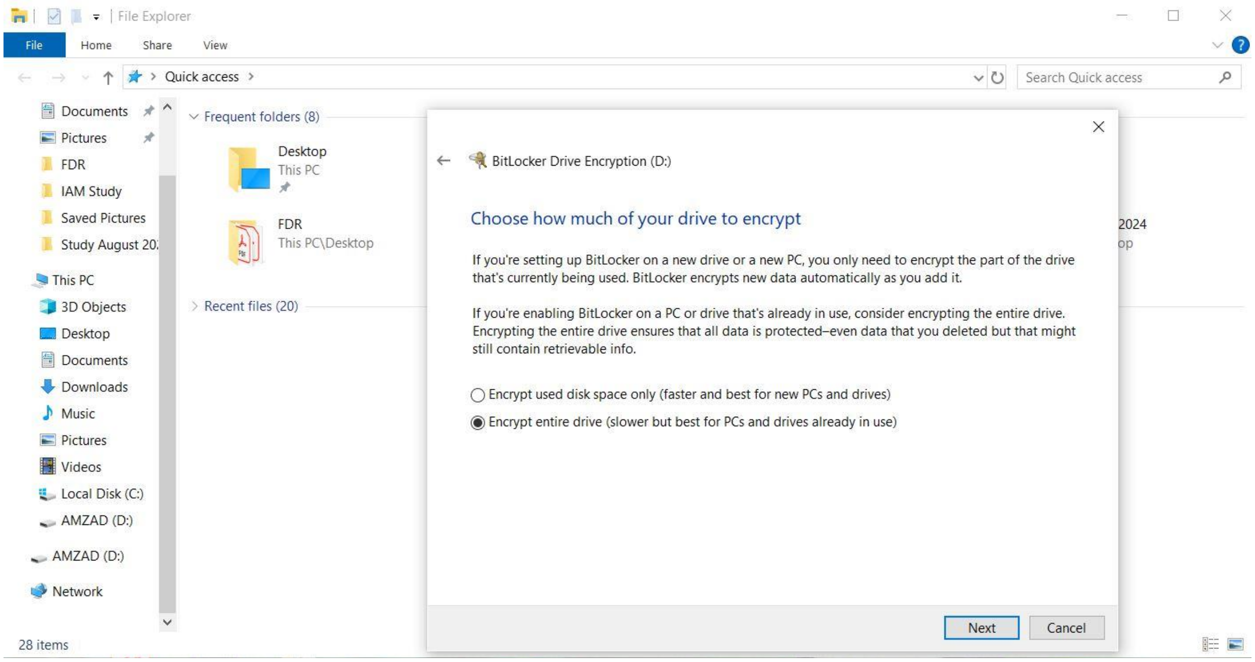
Save BitLocker recovery key as

This PC > Documents

Name	Date modified	Type	Size
CMDworkout	2/12/2024 10:24 AM	File folder	
Custom Office Templates	1/31/2024 6:21 PM	File folder	
Sound recordings	7/15/2024 8:05 PM	File folder	

File name: BitLocker Recovery Key C3038140-FA8C-40AC-8D8B-0D81AC853F29

Save as type: Text Files (*.txt)



BitLocker Drive Encryption (D:)

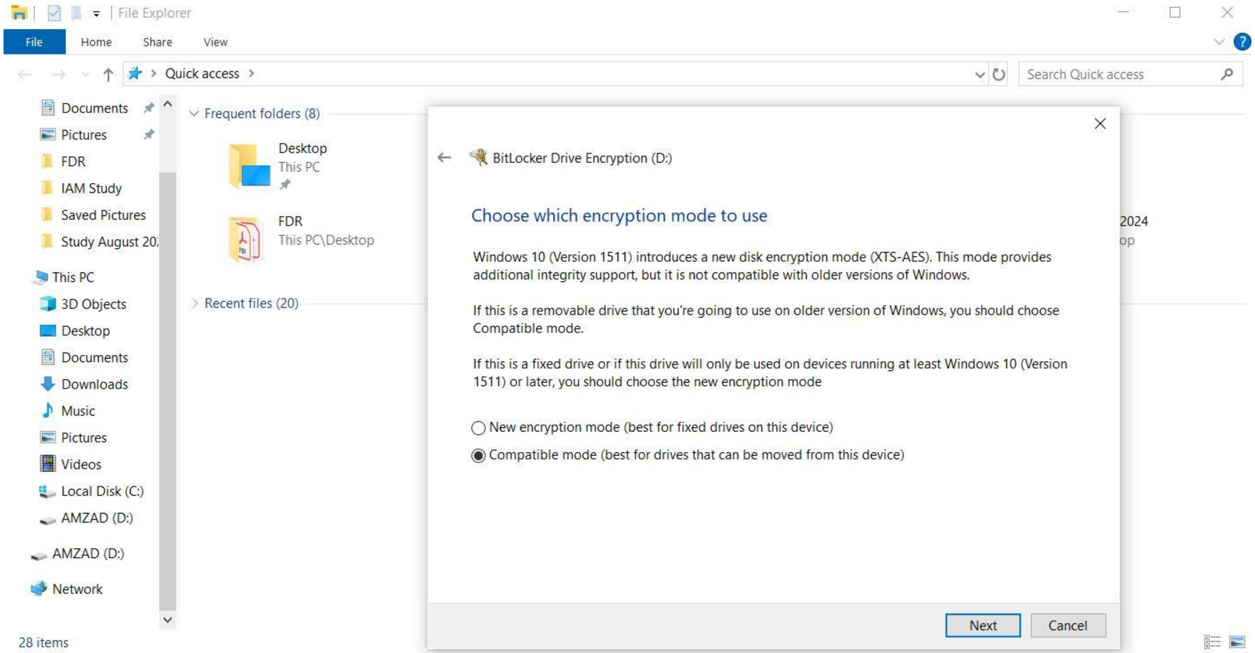
Choose how much of your drive to encrypt

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)



BitLocker Drive Encryption (D:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

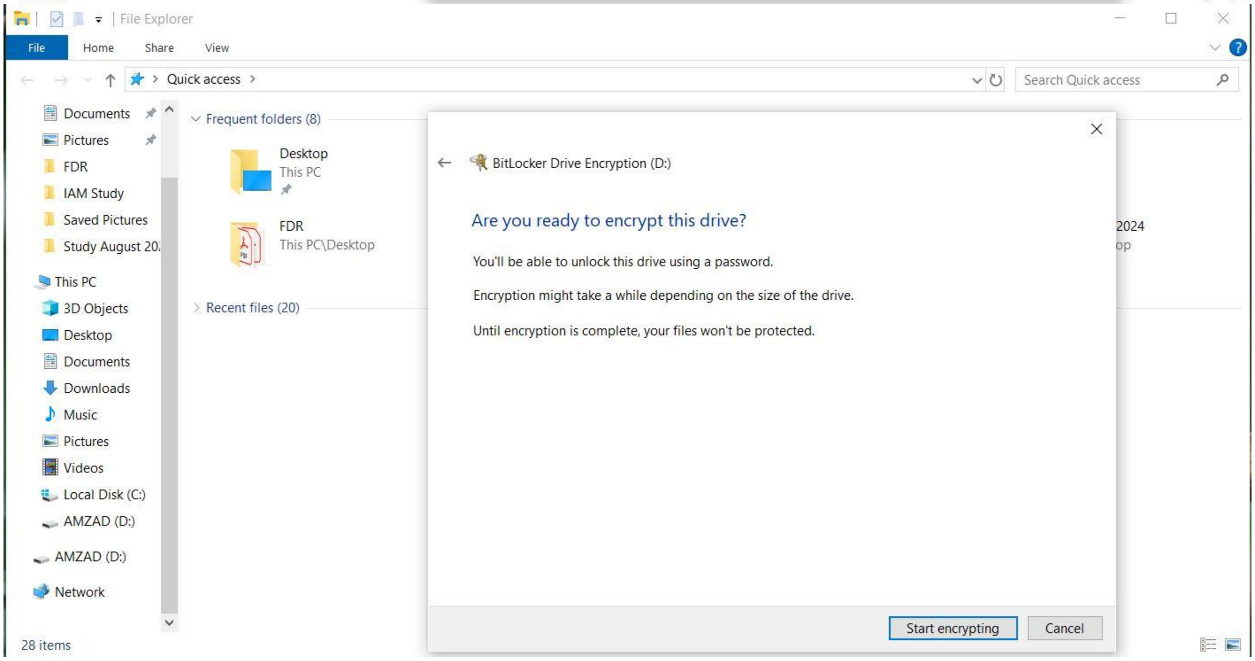
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)

● Compatible mode (best for drives that can be moved from this device)

Next | Cancel



BitLocker Drive Encryption (D:)

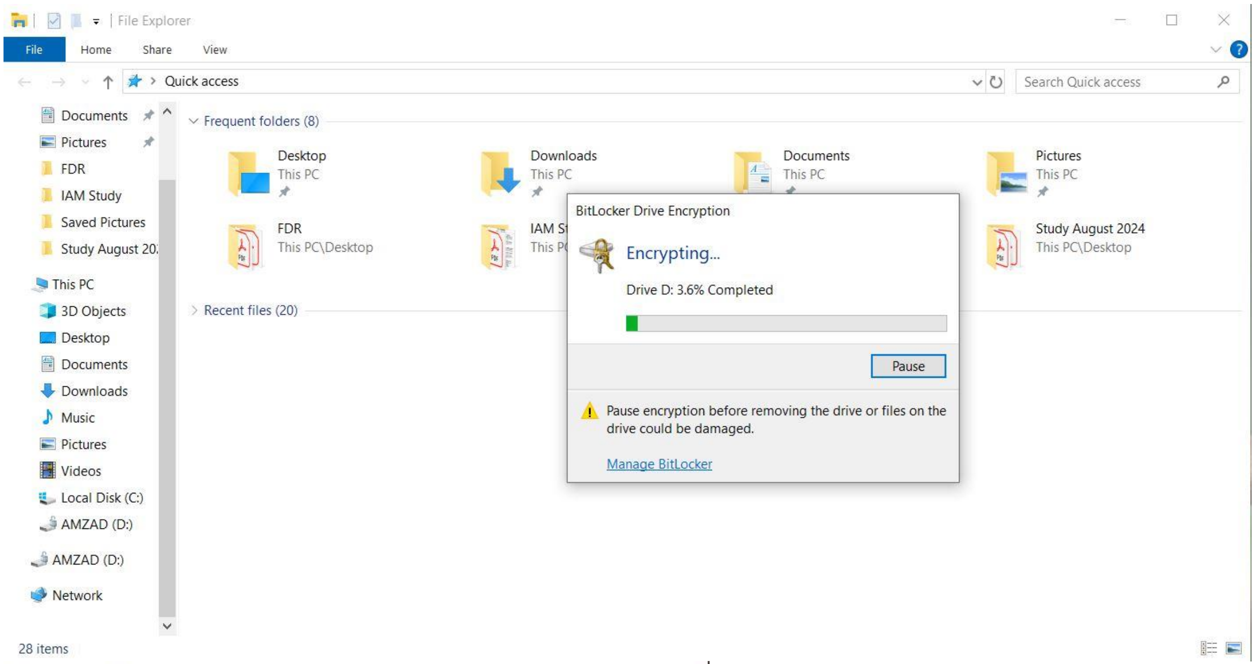
Are you ready to encrypt this drive?

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.

Start encrypting | Cancel

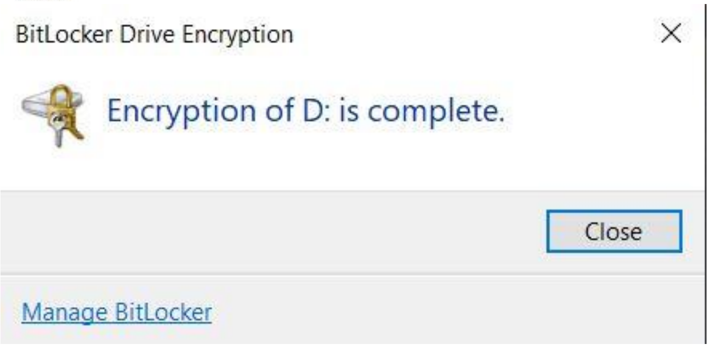


BitLocker Drive Encryption

Encrypting...

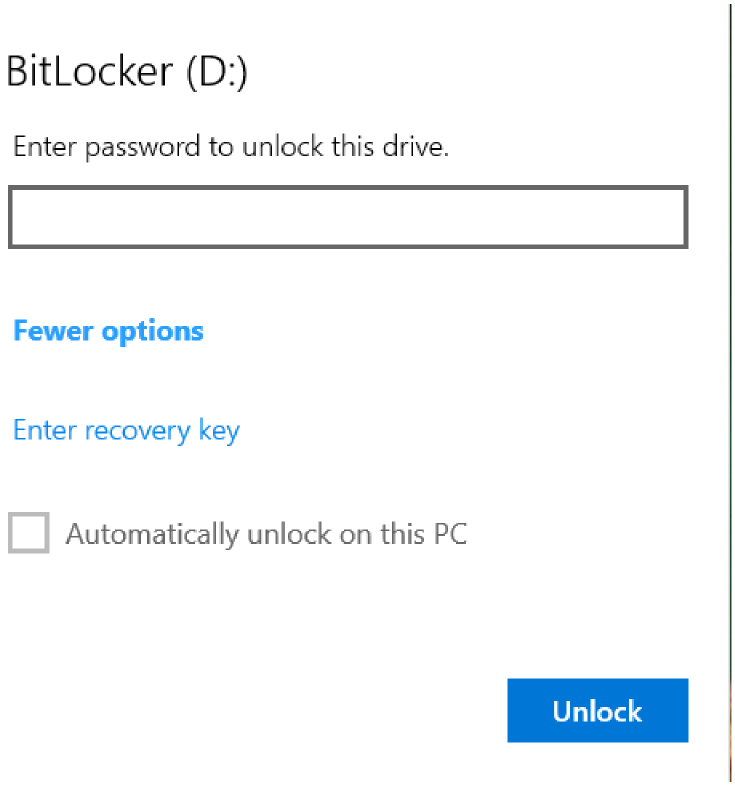
Drive D: 3.6% Completed

Pause encryption before removing the drive or files on the drive could be damaged.



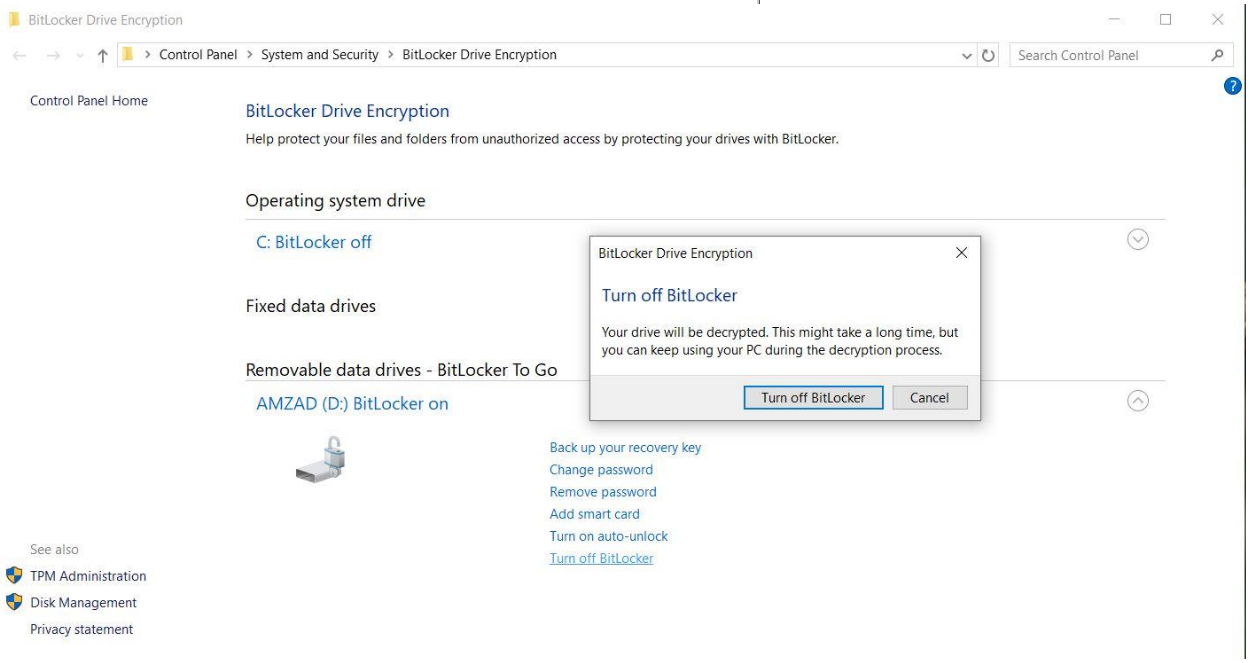
BitLocker Drive Encryption

Encryption of D: is complete.



BitLocker (D:)

Enter password to unlock this drive.



BitLocker Drive Encryption
Control Panel > 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

C: BitLocker off

Fixed data drives

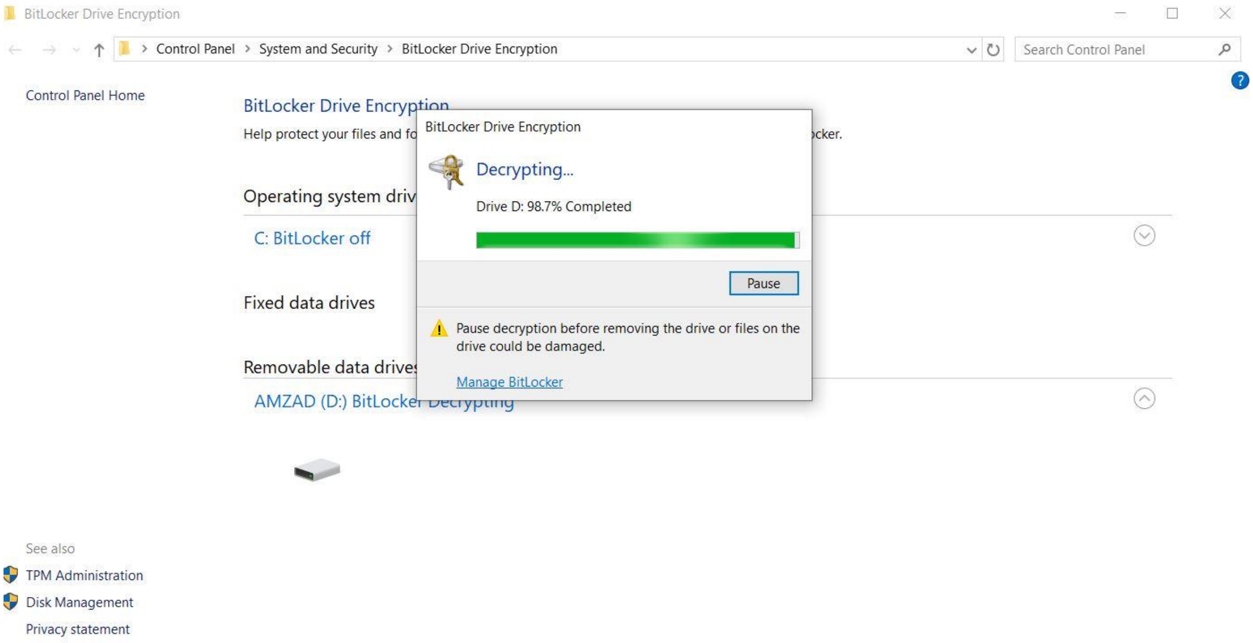
Removable data drives - BitLocker To Go

AMZAD (D:) BitLocker on

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.


BitLocker Drive Encryption
Control Panel > System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and fo… …cker.

Operating system driv…

C: BitLocker off

Fixed data drives

Removable data drives

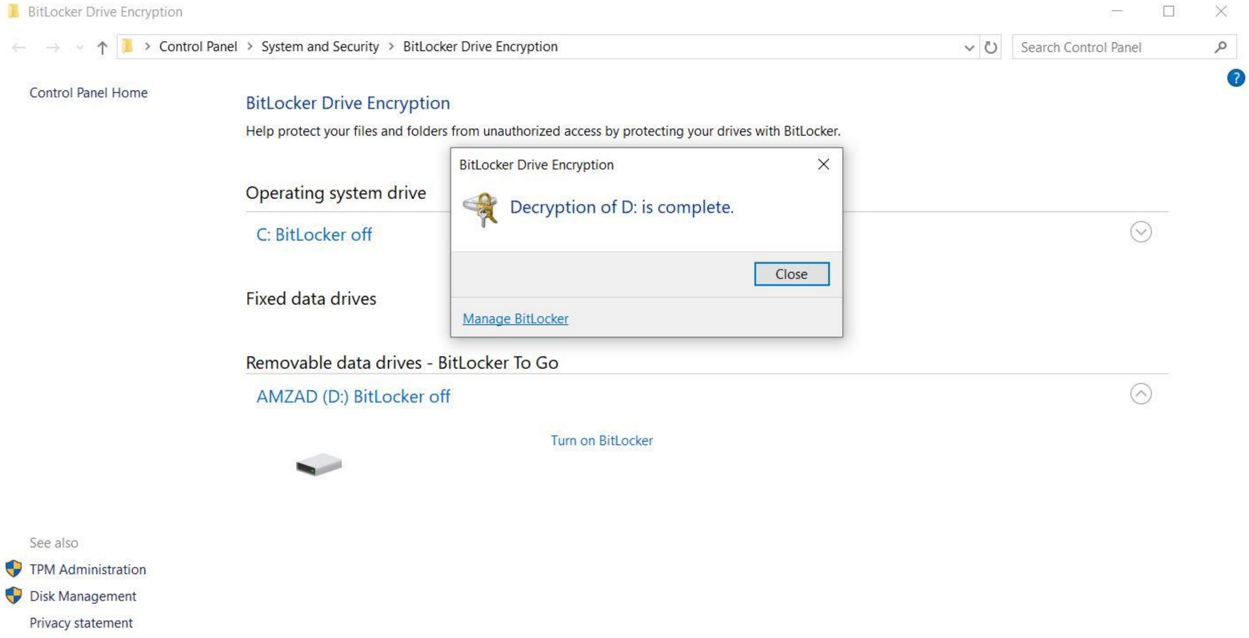
AMZAD (D:) BitLocker Decrypting

BitLocker Drive Encryption

Decrypting...

Drive D: 98.7% Completed

⚠ Pause decryption before removing the drive or files on the drive could be damaged.


BitLocker Drive Encryption
Control Panel > 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

C: BitLocker off

Fixed data drives

Removable data drives - BitLocker To Go

AMZAD (D:) BitLocker off

BitLocker Drive Encryption

Decryption of D: is complete.