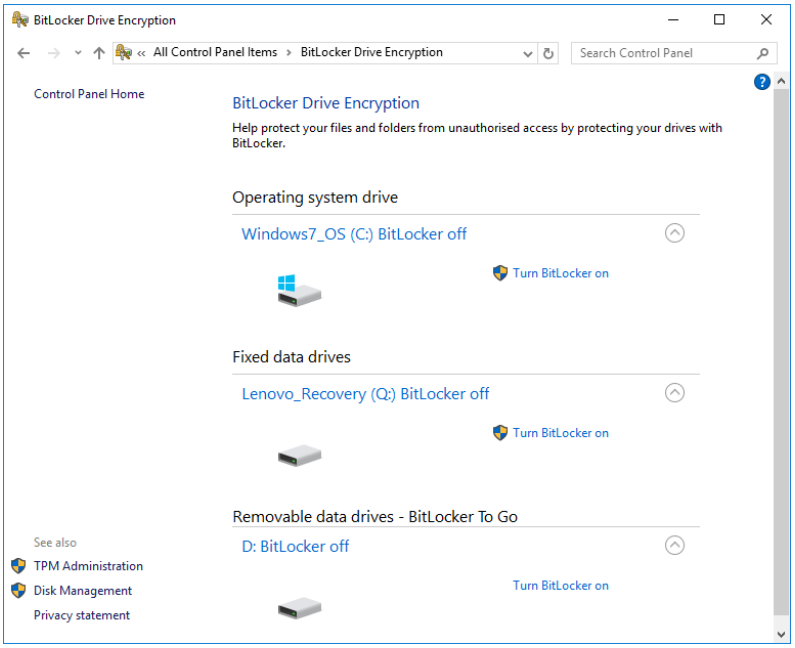
How to encrypt your devices with Windows BitLocker step by step guide

1. Starting the encryption process

The Encryption process must be started from an account with Administrative access.

To access the BitLocker Drive encryption window, right-click on the Drive to encrypt in File Explorer and click "Turn BitLocker on" or Open **Control Panel** by typing it in at the start menu and navigate to **System and Security** and then **BitLocker Drive Encryption**.

The BitLocker Drive Encryption Window will open up as follows:



There are two types of BitLocker encryption you can enable, depending upon the type of disk:

- **BitLocker Drive Encryption:** used for internal Disks, this is the "Full disk encryption" feature that will encrypt an entire drive.

  Once turned on, BitLocker will decrypt the drive and load Windows. The encryption is otherwise seemingless – your files will appear like they normally would on an unencrypted system, but they're stored on the disk in an encrypted form. You can also encrypt other drives in a computer, not just the operating system drive, if you ha vemore than one hard drive in your local machine.

- **BitLocker To Go:** External drives, such as USB flash drives and external hard drives can be encrypted with BitLocker To Go. You'll be prompted for your unlock method – for example, a password when you connect the drive to your computer. Please note - if someone doesn't have the unlock method (ie they forget the password), then they won't be able to ccess the files on the drive.

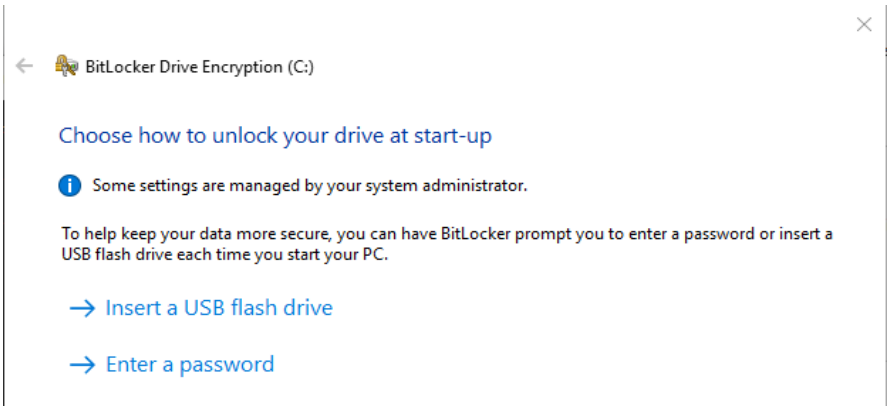
2. Choose an unlock method

Next, you'll see the "**Choose how to unlock your drive at start-up**" screen. You can select several different ways of unlocking the drive. If your computer doesn't have a TPM, you can unlock the drive with a password or by inserting a special USB flash drive that functions as a key.

If your computer does have a TPM, you'll have additional options. For example, you can configure automatic unlocking at start-up – your computer will grab the encryption keys from the TPM and automatically decrypt the drive.

You could also secure it in other ways – i.e., you could provide a PIN at start-up. That PIN would unlock the strong decryption key stored in the TPM and unlock the drive.

Choose your preferred unlock option and follow the instructions in the next screen to set it up.



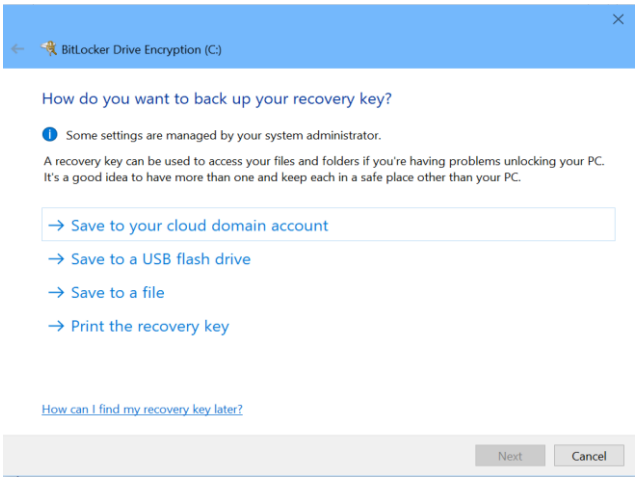
3. Back up your recovery key

BitLocker will provide you with a recovery key. This key can be used to access your encrypted files if you ever lose your main key — for example, if you forget your password or if the computer with the TPM dies and you have to remove the drive. You can save the key to a file, print it, store it on a USB flash drive, or save it to your Microsoft account.

If you back up the recovery key to your Microsoft account, you can access the key later at https://onedrive.live.com/recoverykey .

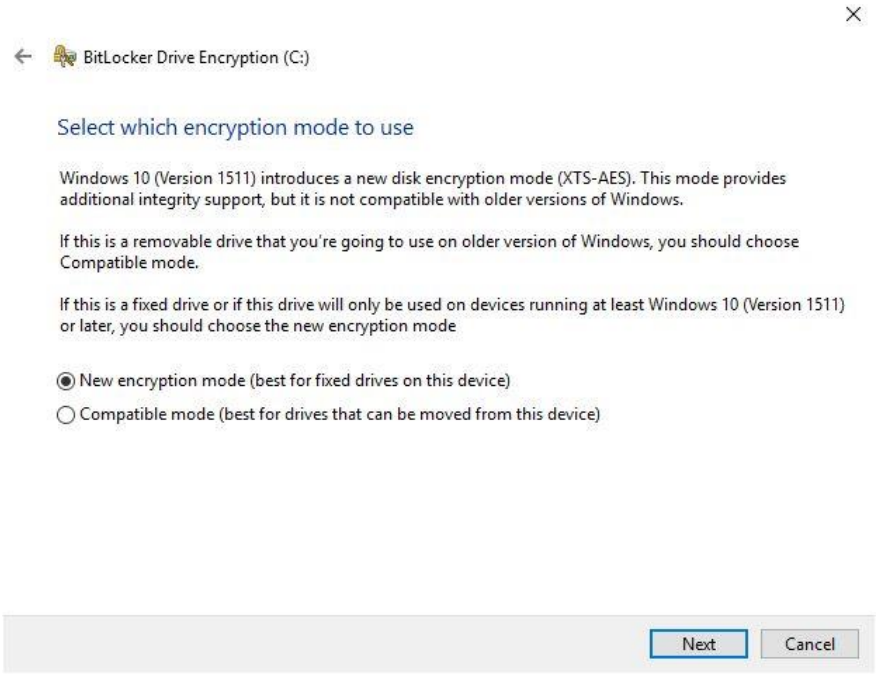
If you are using Azure Active Directory, then the key can be stored with your Azure AD account. Be sure to keep this key safe — if someone gains access to your key, they could decrypt your drive and bypass the encryption.

We would advise you to think about saving it in multiple locations as if you lose this recovery key and are unable to use your main unlock method, your encrypted files will be lost forever.



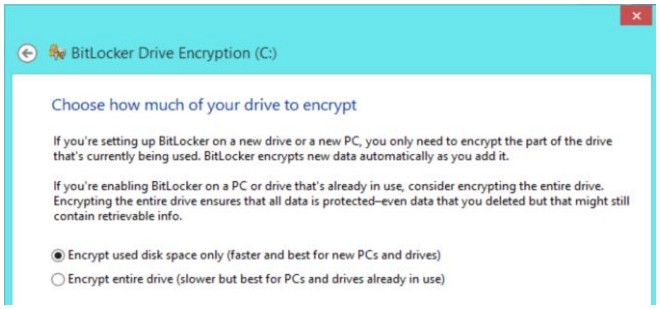
4. Choose the encryption mode

In Windows 10 there is a new encryption mode for BitLocker which isn't compatible with previous Windows versions. If you are encrypting a removable drive that you may need to use with older versions of Windows, you should select the "Compatible Mode". If not, you should choose the "New Encryption Mode".



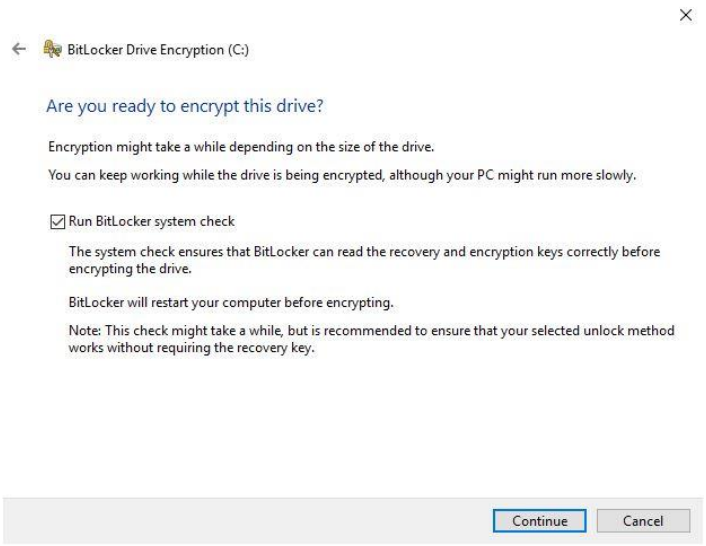
5. Encrypt the drive

On clicking Next, you will be prompted to choose how much of your drive to encrypt. The options are to encrypt the whole drive or just the used space. In most situations you should select to encrypt the entire drive. If you are however encrypting a brand new computer, and to save time, you can select to only encrypt used space.



With either method, BitLocker will automatically encrypt new files as they are added to the device.

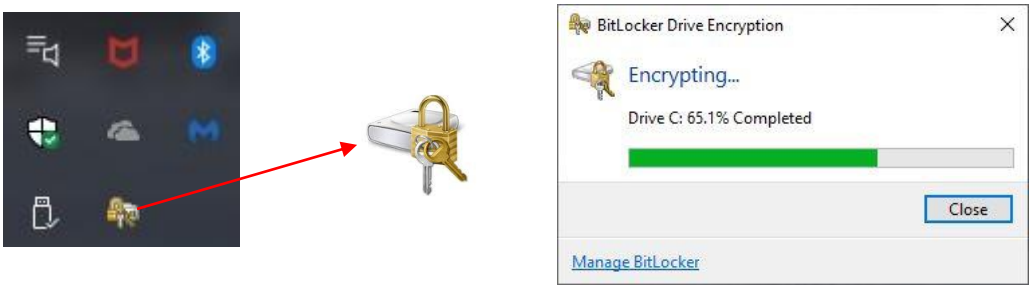
On clicking Next, you will be prompted to run a BitLocker system check and reboot your computer.



6. Encryption progress

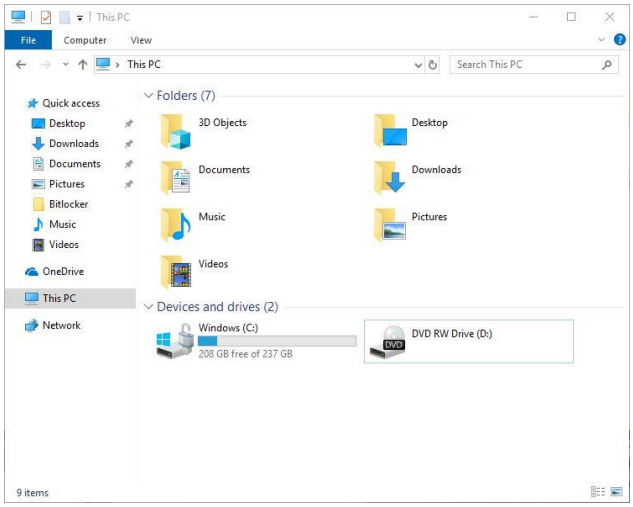
After the computer boots back up for the first time, the encryption process will start. The time it takes will depend upon the size and type of the device being encrypted. For a 256 GB SSD disk, this takes less than 30 minutes. But for a 1 TB hard disk, it can take a couple of hours.

Check the BitLocker Drive Encryption icon in the system tray to see its progress.

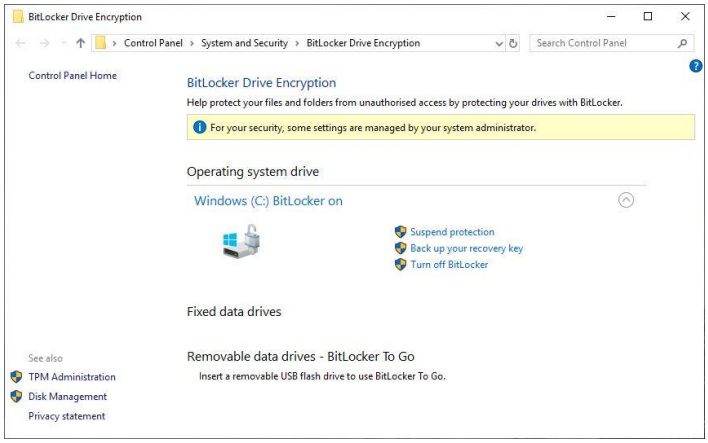


You can continue using your computer while it's being encrypted, but it will perform more slowly, and you will also slow down the encryption process, so this is best to avoid if possible.

Once completed, the status will change to "BitLocker On" for the device status in the BitLocker control panel.

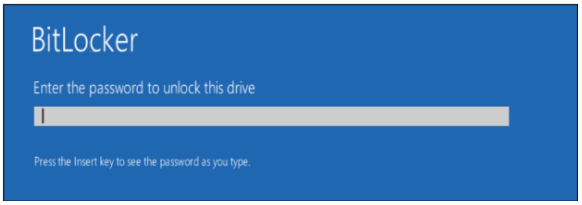


In File Explorer you can see the unlocked padlock icon attached to the drive, indicating that BitLocker is enabled on the device and it is currently unlocked.



Using an encrypted device

When the computer starts, Windows loads from the System Reserved Partition, and the bootloader will retrieve the unlock authentication either from the TPM chip, or by prompting the user for an unlock method if no TPM is present. So if prompted, you should enter the password or PIN, or connect a USB flash drive.



If you are unable to use your unlock method (e.g. your PC has failed or you've forgotten your password), press Escape and you will be prompted to enter the recovery key.

Once the authentication has been verified, your device will then boot normally and you will be able to use it as usual, with the knowledge that data is held on the encrypted drive.

Managing a BitLocker encrypted drive

You can manage a locked drive from the BitLocker control panel window, for example if you want to change the password, turn off BitLocker or back up your recovery key. Right click the encrypted drive in question and select Manage BitLocker to go directly to it.

For further information - please see Microsoft's official BitLocker FAQ quick answer general questions covering all things BitLocker.

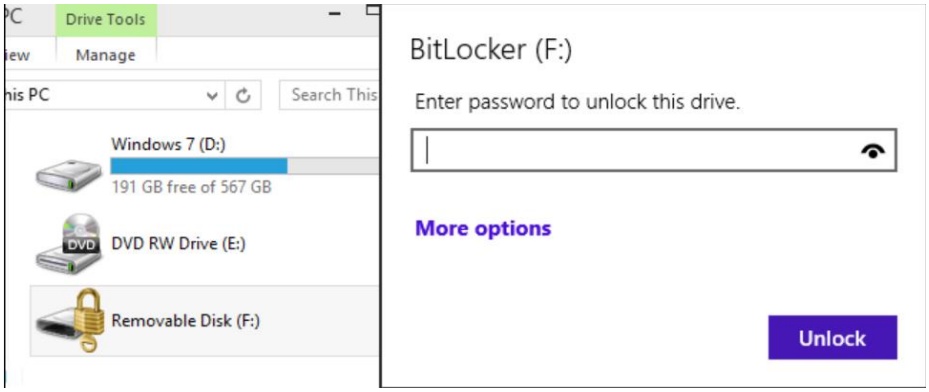
Encrypting a removable drive

In addition to encrypting an internal disk in your PC or laptop, BitLocker can also encrypt removable devices, such as USB flash drives, and this is called BitLocker To Go.

If you choose to encrypt a removable drive with BitLocker To Go, you'll see a similar wizard but your drive will be encrypted without any rebooting required. It is recommended to select the "Compatible Mode" for the encryption, as otherwise the device will not be usable in pre Windows 10 devices.

Don't remove the drive while it's being encrypted, as this may corrupt the device and data on it.

When you connect the encrypted drive to a computer, you'll be prompted to provide a password, or smart card, whichever method you've chosen to unlock the removable device. Drives protected with BitLocker are identified with a lock icon in Windows Explorer or File Explorer.



If a removable device is used regularly in a computer, it is possible to 'remember' the BitLocker key on that device, so that the user will not need to enter it each time. But if someone inserts it into a different device, they would need to enter this before they are able to access the contents.