Turning on BitLocker drive encryption on Windows computers

Before you start a couple of **VERY** important notes...

a) Make sure you have **backups** before you start just in case anything goes wrong (as it's much harder, usually impossible, to recover data from an encrypted drive - as you would hope and expect).
b) Make sure you **keep a safe copy of the encryption key** And please provide a copy for the IT Office to store for use in the event of a problem or, if you choose to let Microsoft keep it, make sure you know your login details for Microsoft.

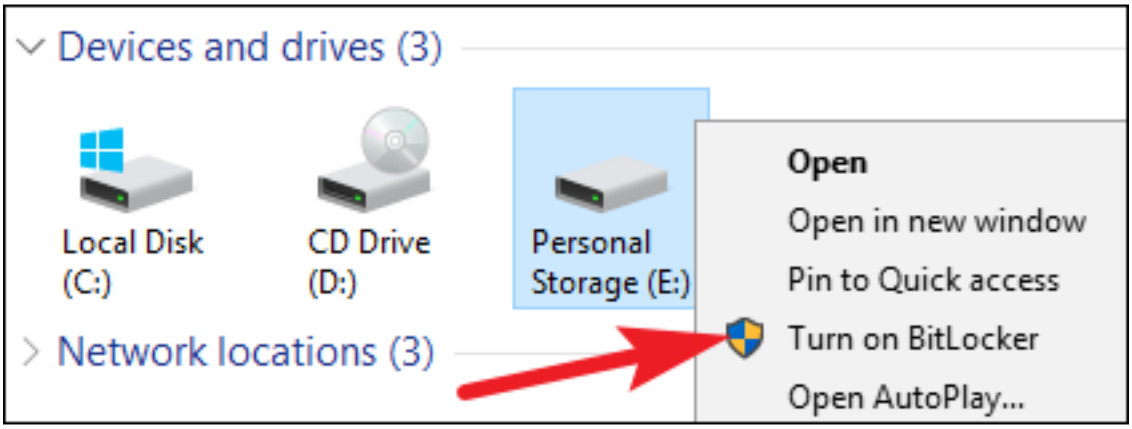
If you forget the passwords and can not recover a copy of your key you will **loose all your files** (which is another reason to keep backups).

If you reset BitLocker and a new encryption key is set - please remember to provide a copy to the IT Office

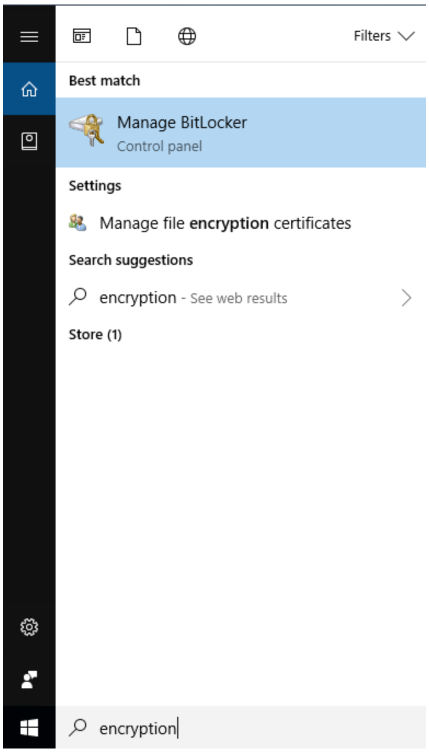
Windows 7, 8 and 10 have BitLocker Built in, this can be used to encrypt the hard drive. It just needs to be activated following the steps shown below.

1) Enable BitLocker for a Drive

The easiest way to enable BitLocker for a drive is to right-click the drive in a File Explorer window, and then choose the "**Turn on BitLocker**" command.



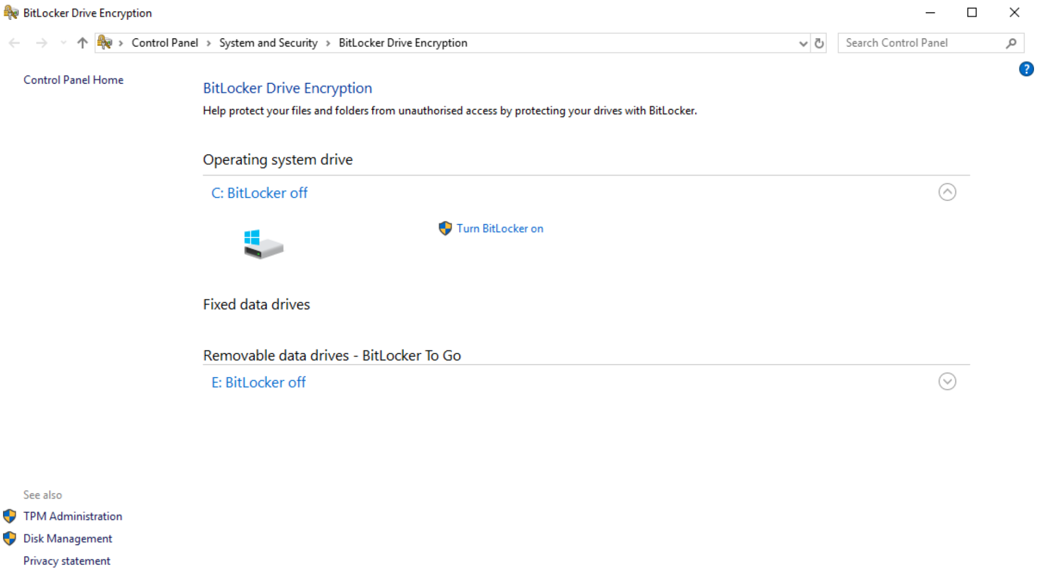
If you don't see this option on your context menu. Then click on the windows icon and where it says "Type here to search" type in "encryption" and click on "Manage BitLocker" from the list of options that appears.



It’s just that simple. The wizard that pops up walks you through selecting several options, which we’ve broken down into the sections that follow.

2) Turn BitLocker On

The first screen you’ll see in the “**BitLocker Drive Encryption**” Allows you to choose the Drive to Encrypt.


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 unauthorised access by protecting your drives with BitLocker.

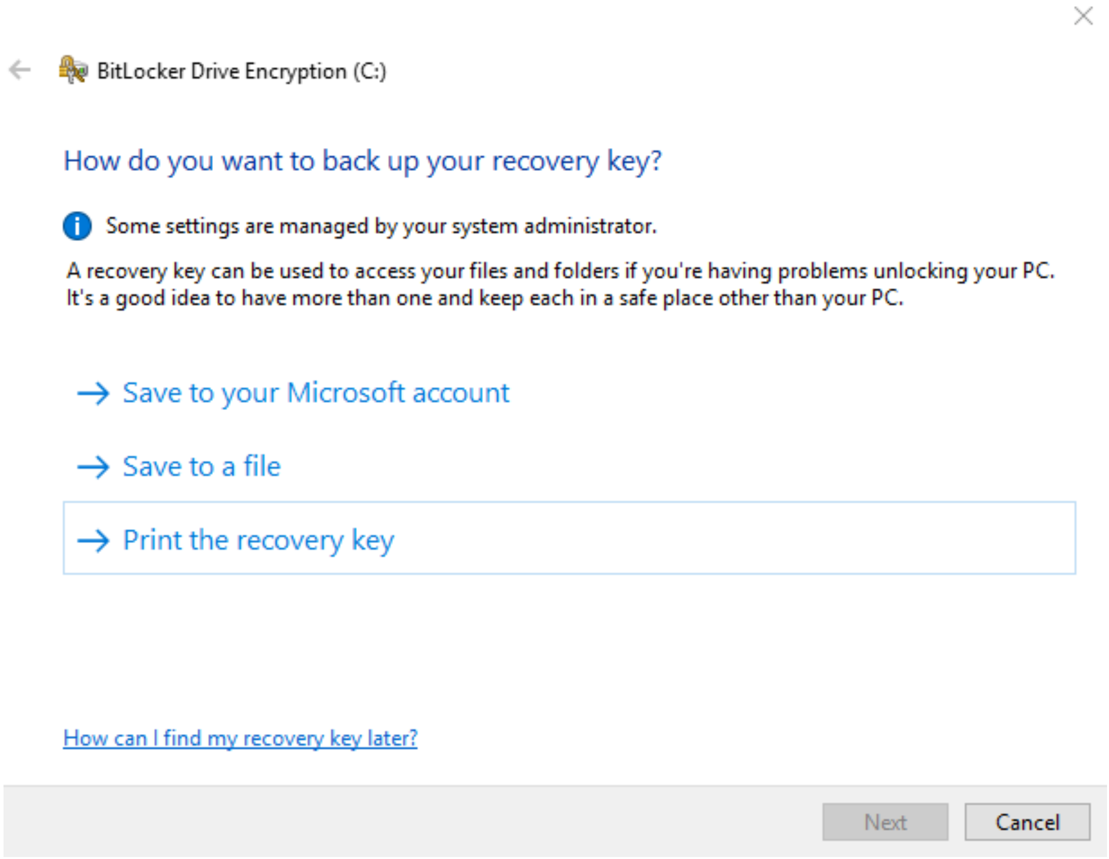
Click “**Turn Bitlocker on**”.

BitLocker will start and check the computers configuration and then prompt you to back up the recovery key.

3) Back Up Your Recovery Key

BitLocker provides you with a recovery key that you can use to access your encrypted files should you ever lose your main key—for example, if you forget your password or if the PC dies and you have to access the drive from another system.

We recommend you print a copy of the recovery key as a PDF. Please keep a copy of this somewhere safe and it is advisable to give a copy to the IT Office where we will store it safely.



BitLocker Drive Encryption (C:)

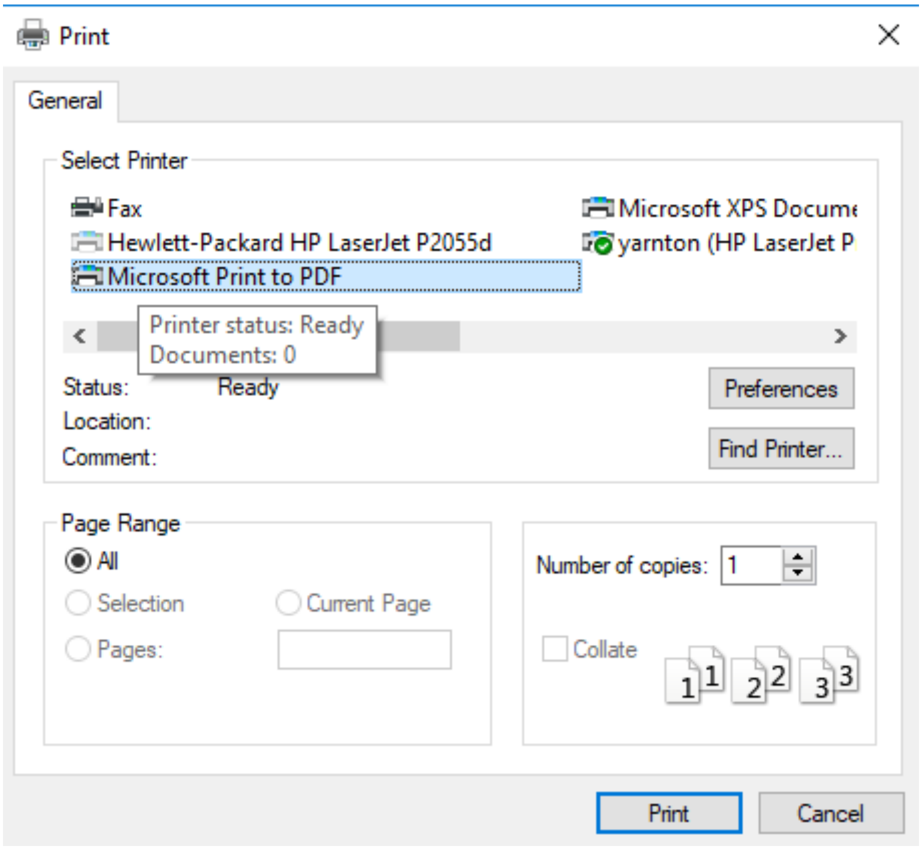
How do you want to back up your recovery key?

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
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel

To save as a PDF Click on “**Print the recovery key**” At the print window in the **Select Printer** window Select your PDF creator – this will be either Microsoft Print to PDF or Nuance PDF.



Microsoft Print to PDF

Printer status: Ready
Documents: 0

Status: Ready
Location:
Comment:

● All

Number of copies: 1

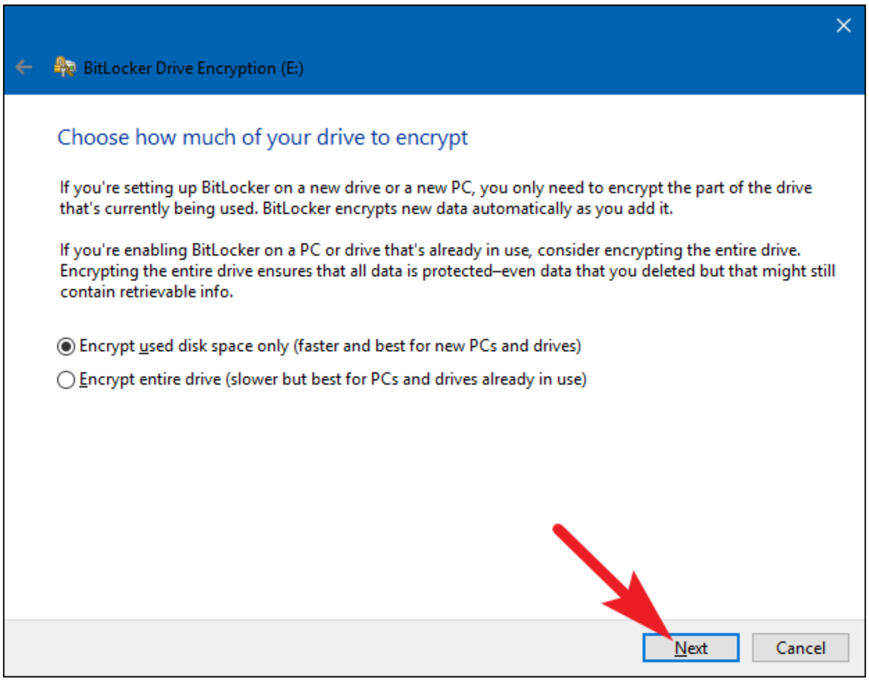
Click “**Print**” and you get an option as to what to save the file as and where to save it. Please make a note of this, After printing to PDF Check that you can find the file and that it opens and contains an identifier and the recovery key. You are then returned to the “how do you want to back up your recovery key? Window.

You can also back up your recovery key multiple ways if you want. Just click each option you want to use in turn, and then follow the directions. When you’re done saving your recovery keys, click “Next” to move on.

4) Encrypt and Unlock the Drive

BitLocker automatically encrypts new files as you add them, but you must choose what happens with the files currently on your drive. You can encrypt the entire drive—including the free space—or just encrypt the used disk files to speed up the process. These options are also the same whether you’re encrypting a system or non-system drive.

If you’re setting up BitLocker on a new PC, encrypt the used disk space only—it’s much faster. As you’re setting BitLocker up on a PC you’ve been using for a while, you should encrypt the entire drive to ensure no one can recover deleted files.



BitLocker Drive Encryption (E:)

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)

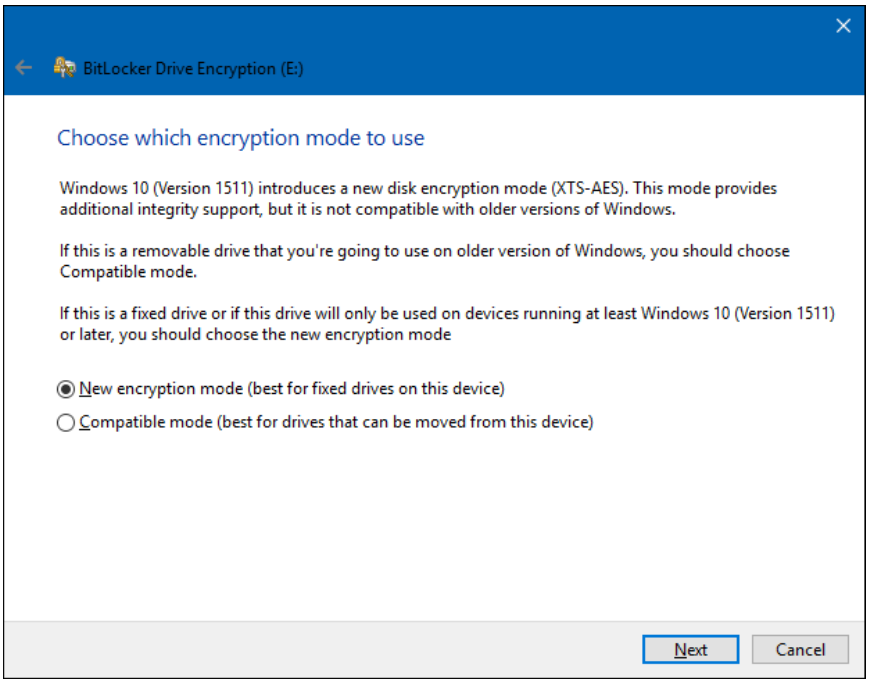
○ Encrypt entire drive (slower but best for PCs and drives already in use)

When you've made your selection, click the "Next" button.

5) Choose an Encryption Mode (Windows 10 Only)

If you're using Windows 10, you'll see an additional screen letting you choose an encryption method. If you're using Windows 7 or 8, skip ahead to the next step.

If you know the drive you're encrypting is only going to be used on Windows 10 PCs, go ahead and choose the "**New encryption mode**" option. If you think you might need to use the drive with an older version of Windows at some point (especially important if it's a removable drive), choose the "**Compatible mode**" option.



BitLocker Drive Encryption (E:)

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.

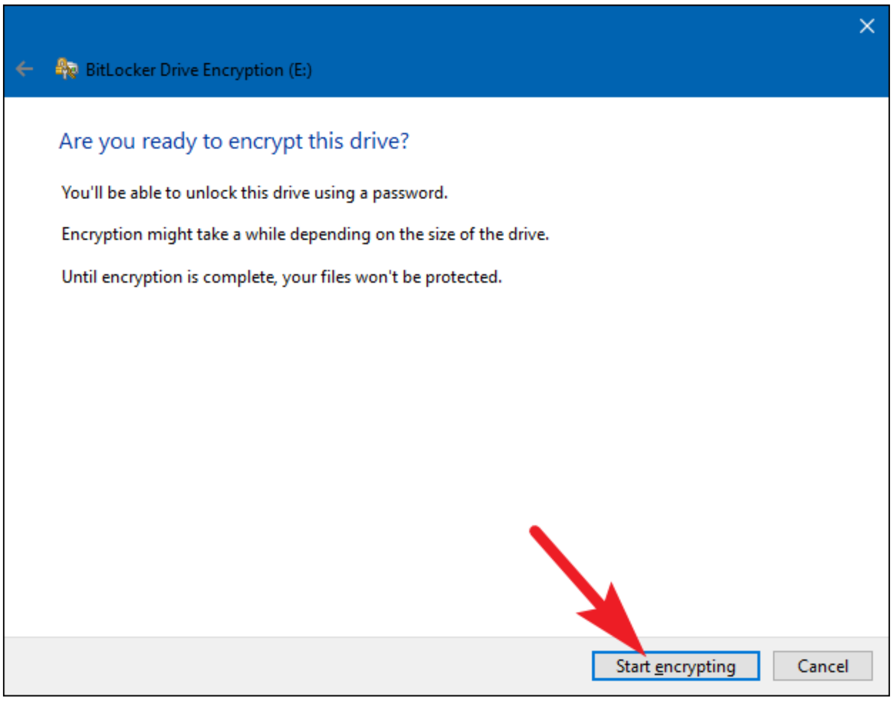
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

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)

Whichever option you choose (and again, these are the same for system and non-system drives), go ahead and click the “**Next**” button when you’re done, and on the next screen, click the “**Start Encrypting**” button.



BitLocker Drive Encryption (E:)

Are you ready to encrypt this drive?

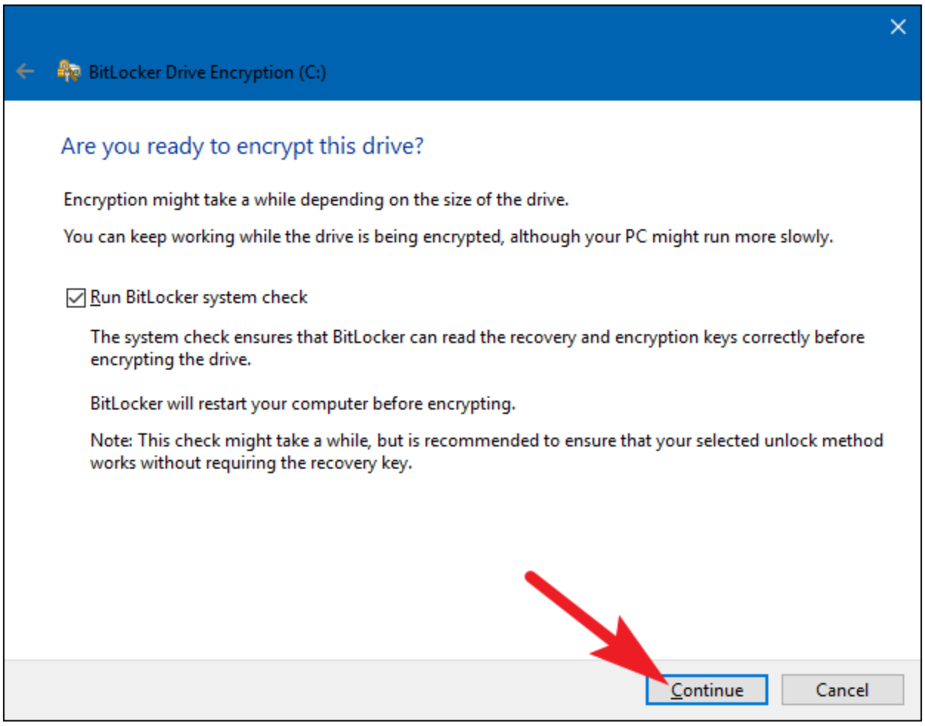
You'll be able to unlock this drive using a password.

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

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

6) Finishing Up

The encryption process can take anywhere from seconds to minutes or even longer, depending on the size of the drive, the amount of data you’re encrypting, and whether you chose to encrypt free space.
If you’re encrypting your system drive, you’ll be prompted to run a BitLocker system check and restart your system. Make sure the option is selected, click the “**Continue**” button, and then restart your PC when asked. After the PC boots back up for the first time, Windows encrypts the drive.



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.

If you’re encrypting a non-system or removable drive, Windows does not need to restart and encryption begins immediately.

Whatever type of drive you’re encrypting, you can check the BitLocker Drive Encryption icon in the system tray to see its progress, and you can continue using your computer while drives are being encrypted—it will just perform more slowly until the encryption process is completed.