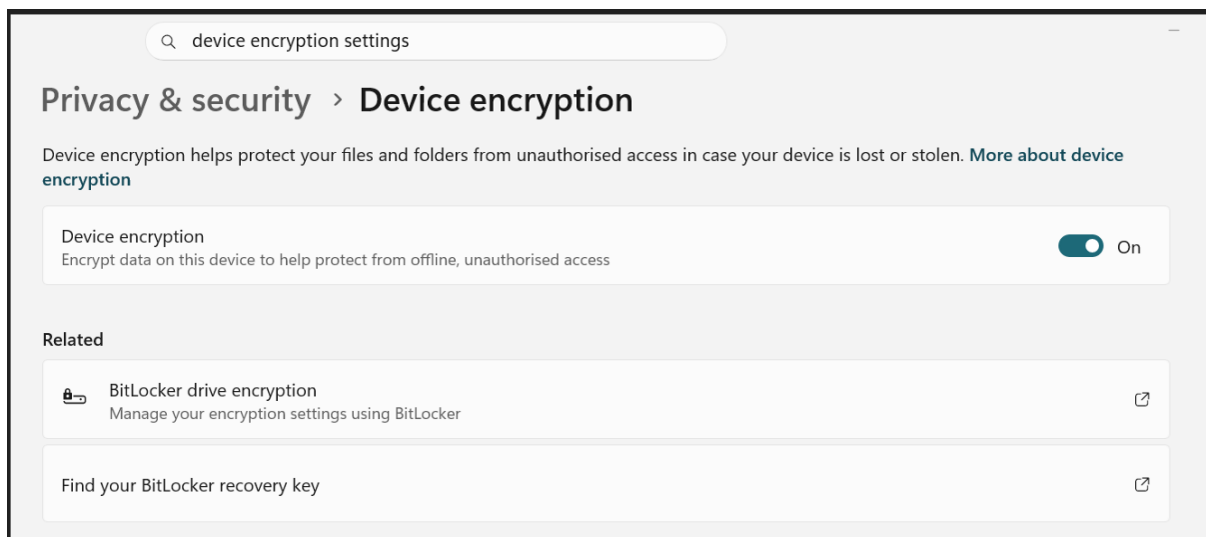


BIT-LOCKER

You need to have a copy of the drive encryption KEY.

Windows 11 Home and Professional come with a feature called Bit Locker. Bit Locker encrypts your Installed Hard Drives. There are options in Settings to turn off Drive encryption.

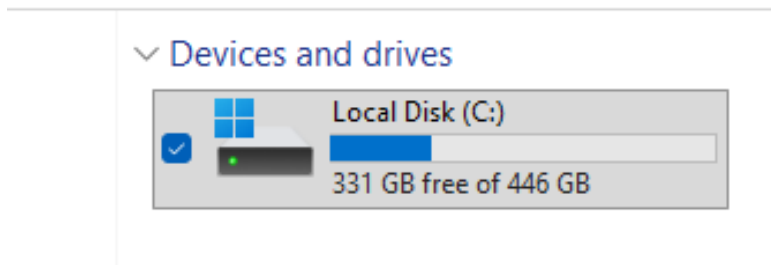
Open Settings and in the search field type “device encryption settings” and you will see the following:



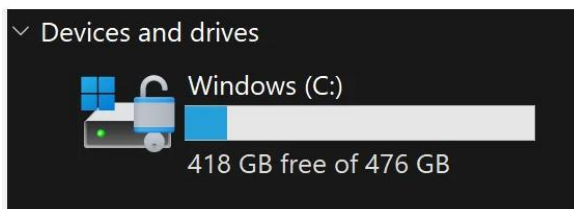
NOTE: Not all Windows 11 Home PC's will have Bit Locker Drive Encryption due to Firmware settings and limitations in the BIOS. If you can't find this setting in Windows 11 Home, your PC does not support Drive Encryption.

To see if your drive is encrypted open File Explorer > This PC and look at the C: Drive. If you see a pad lock then the drive is encrypted.

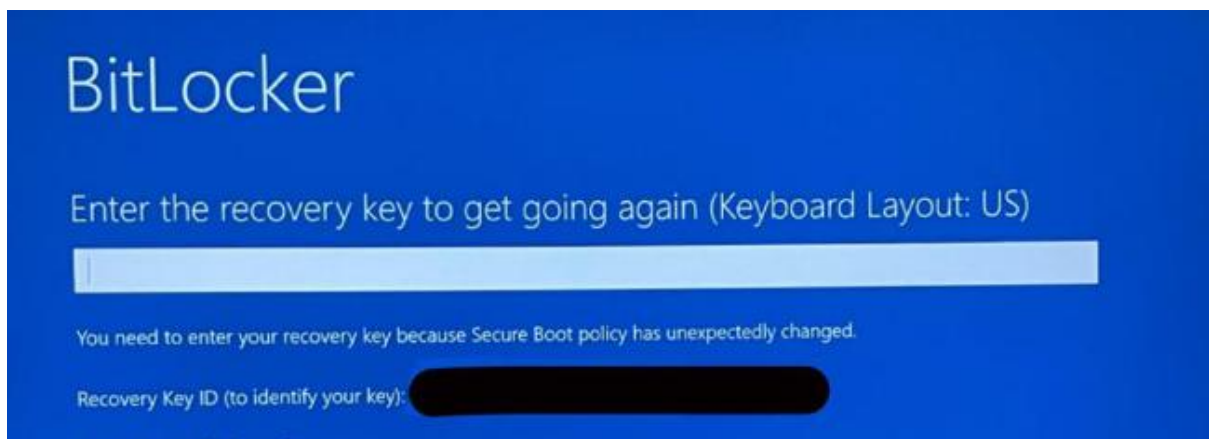
In the example below there is no padlock so the drive is not encrypted.



If the Drive is encrypted you will see this: (Notice the Padlock)



If a fault occurs with your BIOS or the Operating System you may see a notice like this when you turn on your computer:

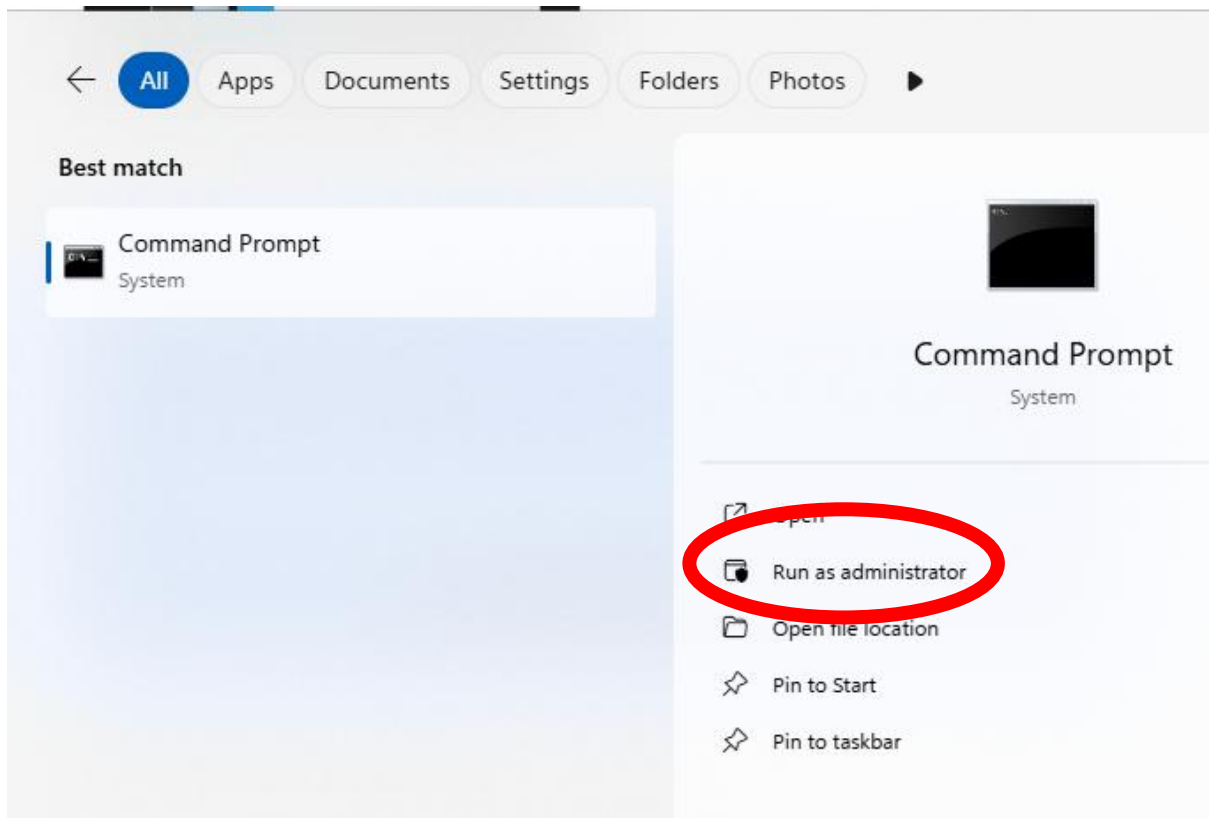


If you are at this blue BitLocker recovery screen, the system will explicitly display a "Recovery key ID". This identifies your hard drive. Match this ID with your list and enter the key.

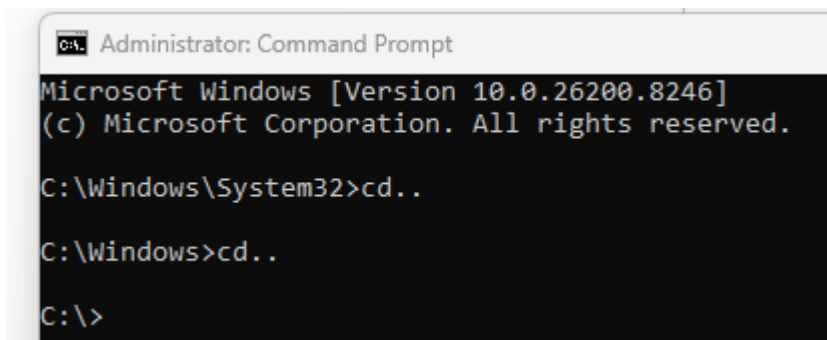
You need to have a copy of the drive encryption KEY.

To find your Recovery Key ID and the Recovery Key you can use the Command Prompt.

1. On your task bar in search type cmd, select Run as administrator.



2. Type the following commands and press Enter:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26200.8246]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd..
C:\Windows>cd..
C:\>
```

cd.. takes you back to the Windows directory
cd.. the second time takes you back to the root directory C:. (This is where your text file will be stored)

Now type this command:

manage-bde -protectors -get C:

(Replace C: with any other drive letter, like D: or E:, as needed).

This command will reveal the Key ID as well as the Recovery Key.

3. To save the output from this command as a text file type the following command:

manage-bde -protectors -get C: > bitlocker.txt

This command will output the results to a text file located in the current directory as shown in cmd. C: if you followed the above instructions about CD..

Example:

C:\manaage-bde -protectors -get D: > bitlocker.txt

BitLocker Drive Encryption: Configuration Tool version 10.0.26100
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: []
All Key Protectors

TPM:

ID: {11175A53-3DBA-4409-9545-89AD8B10FD43}

PCR Validation Profile:

7, 11

(Uses Secure Boot for integrity validation)

Numerical Password:

ID: {3D9F90GG-112C-4D2A-85A2-2B895D5F887D}

Password:

511115-135509-123456-247654-653000-575201-239910-464464

Backup type:

Microsoft account backup

Saved to file

The Recovery key ID is the first part of the ID shown in yellow above.
The Key ID is that big long number after Password. This is the number you have to manually enter when you see the blue screen come up asking for the Bit Locker Key.

Open File Explorer > C: and copy the bitlocker.txt file to a USB or print it.