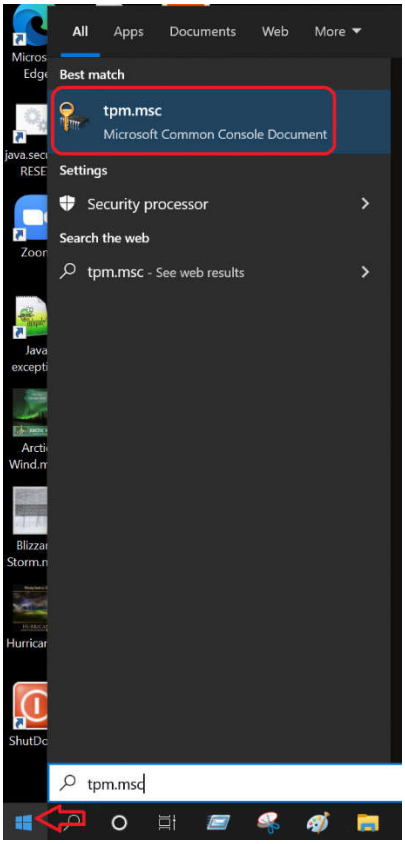
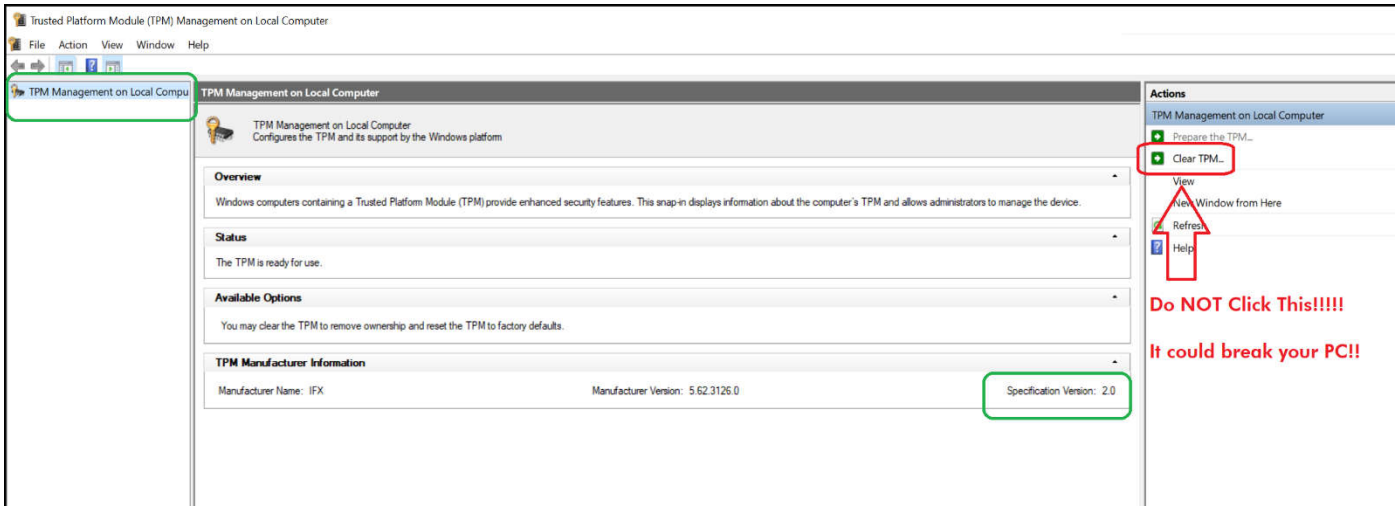
**To see if your PC/Laptop supports Proper drive encryption**

1. Click on Start, type " tpm.msc " and click on that program to run it.




**Warning the next step comes with great risk, please be careful!!!**

2. Click on TPN management on the left-hand side circled in green, notice the specification version lower right hand corners circled in green, Windows 11 only supports version 2.0, Windows 10 supports 1.23 & 2.0, if your specification version shows 1.22 there is a way to still get encryption to work but there's extra work that needs to be done. Do not click on the "clear TPM" if you currently have Bitlocker activated, even if incorrectly, you will completely break and erase your current hard drive! (Please see items in red)

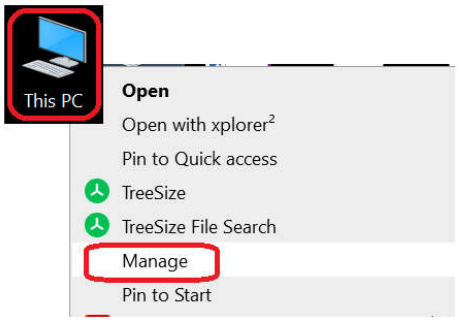


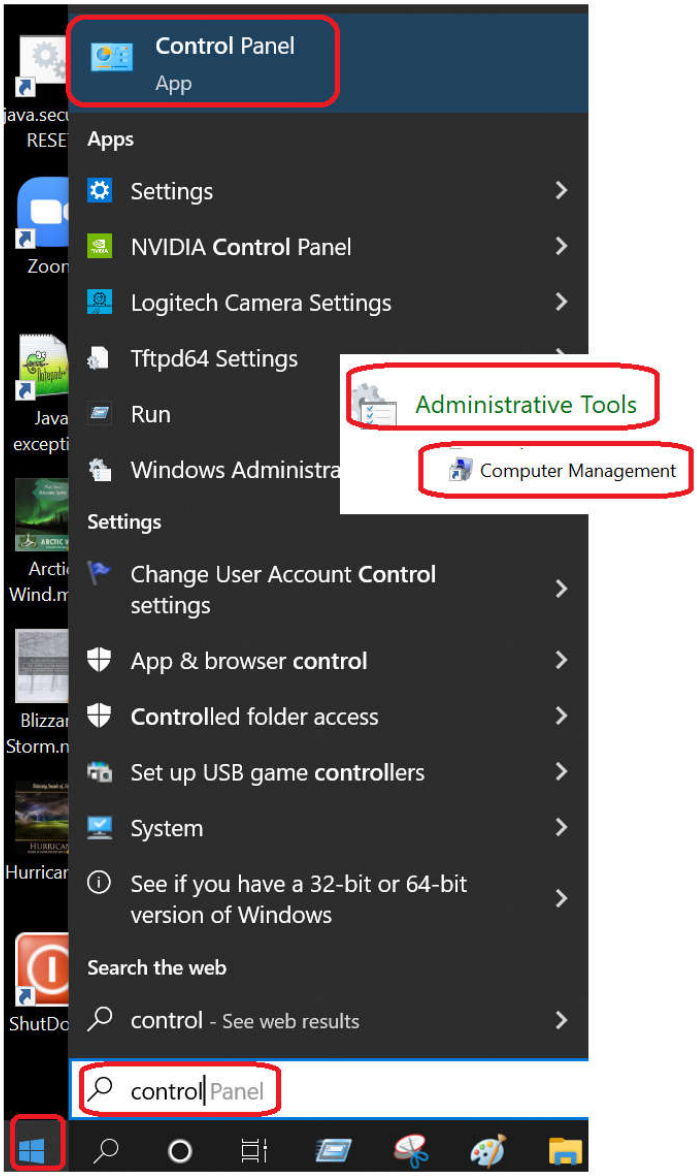
3. Check you HDD type, NVMe, M.2 & SSD are 10 times faster when doing the encryption insall. SATA drives take considerably longer. Check your drive type. Two ways to get there, see below.

**Right click "Thic PC" or "My Computer" icons on your desktop. Then click on "Manage"**

**OR**

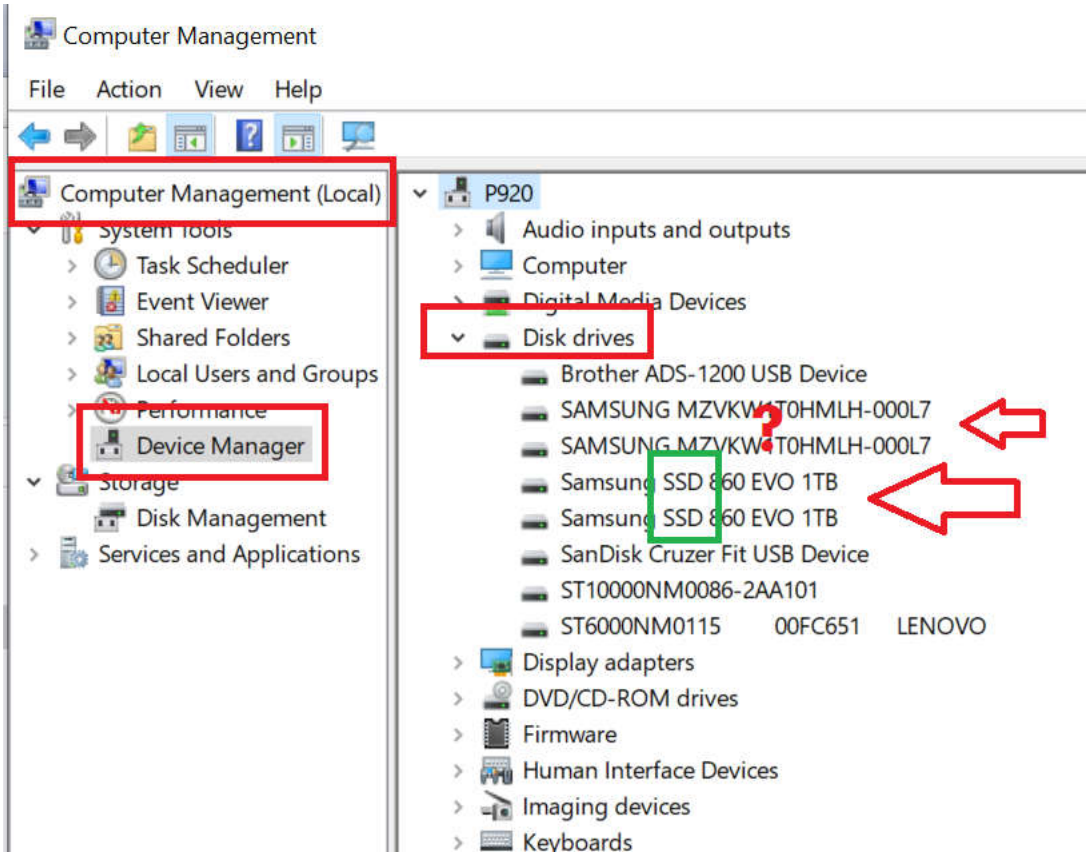
**Click on Windows Start button and Type: control panel, then click on "Administrative Tools" then "Computer Management"**




( See Next Page )

4. Now, inside “Computer Management” go down to “Device Manager” , Then “Disk Drives”. See what type of drives you have. Monarch will need this information for an accurate quote. As you can see in the example below, The top 2 Samsung drives are actually NVMe drives (red ? mark), but there’s no way to really tell without looking at the specs. However, the bottom 2 Samsung drives have “SSD” directly in the name (squared in green). With that said, if you don’t feel like doing it you can skip this step knowing that SATA and slower drives takes anywhere between ½ to 1Hr longer to encrypt.

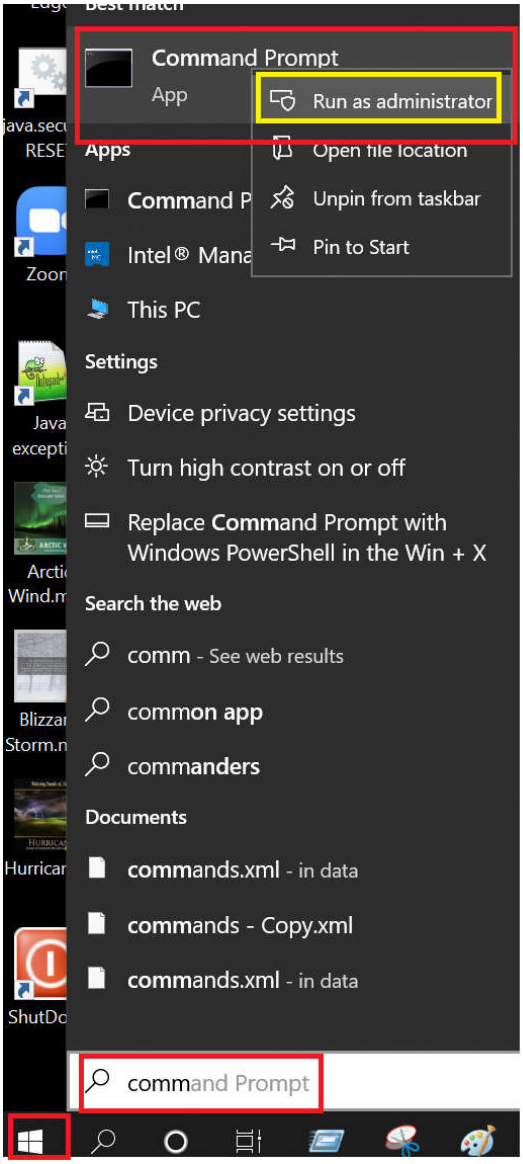


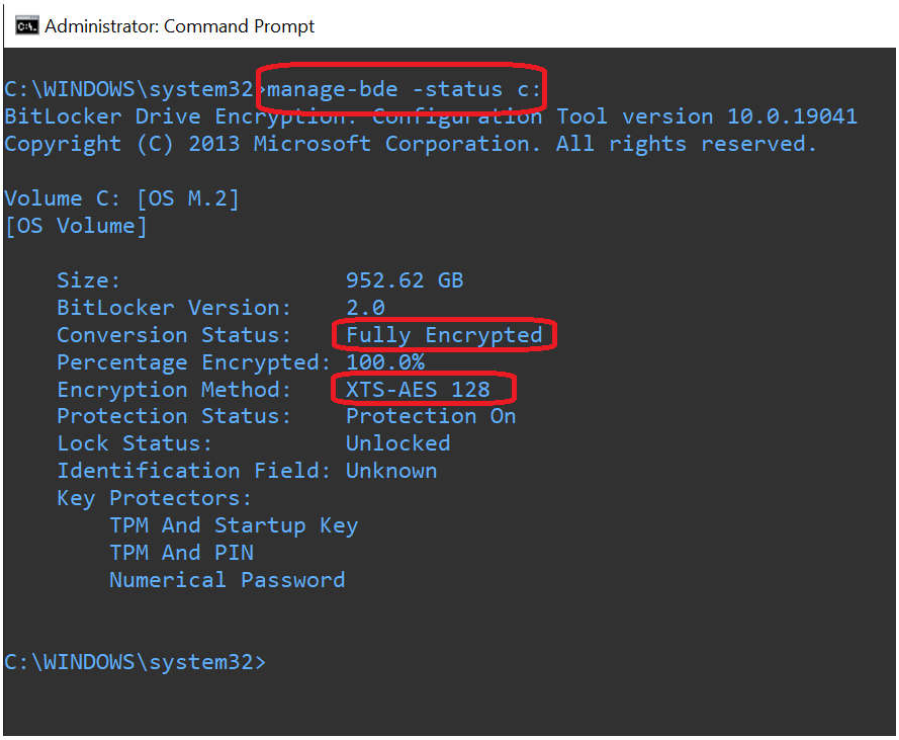

5. Please report this information inside of the ticket for a more accurate quote.

Also: if have already believe you have implemented “Bitlocker” HDD encryption, I hate to inform you, but you haven’t done it correctly for these two reasons :

1. If your computer does not ask you for a password before it even starts to boot, then it INCORRECT!
2. If under any compliance regulations ie.. HIPAA, SOC2, NIST/CMMC, PCI, GLBA ect.. And you used “control-panel, Bitlocker” that is also incorrect as control panel only offers AES-128. The required AES-256 can only be installed using command line CLI. Here’s how to tell
   a. Goto Start, and type “Command”, click on “Command Prompt” right click “Run-as-Admin”
   b. After opening a dos prompt/box as admin type “manage-bde -status c:”

(See Next Page)


Command Prompt
App
Run as administrator
Open file location
Unpin from taskbar
Pin to Start
Apps
Command P
Intel® Mana
This PC
Settings
Device privacy settings
Turn high contrast on or off
Replace Command Prompt with Windows PowerShell in the Win + X
Search the web
comm - See web results
common app
commanders
Documents
commands.xml - in data
commands - Copy.xml
commands.xml - in data
command Prompt


Administrator: Command Prompt
C:\WINDOWS\system32>manage-bde -status c:
BitLocker Drive Encryption: Configuration Tool version 10.0.19041
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
Volume C: [OS M.2]
[OS Volume]
Size: 952.62 GB
BitLocker Version: 2.0
Conversion Status: Fully Encrypted
Percentage Encrypted: 100.0%
Encryption Method: XTS-AES 128
Protection Status: Protection On
Lock Status: Unlocked
Identification Field: Unknown
Key Protectors:
TPM And Startup Key
TPM And PIN
Numerical Password
C:\WINDOWS\system32>