Worcester Polytechnic Institute
Department of Computer Science

Module 1: Windows Bitlocker

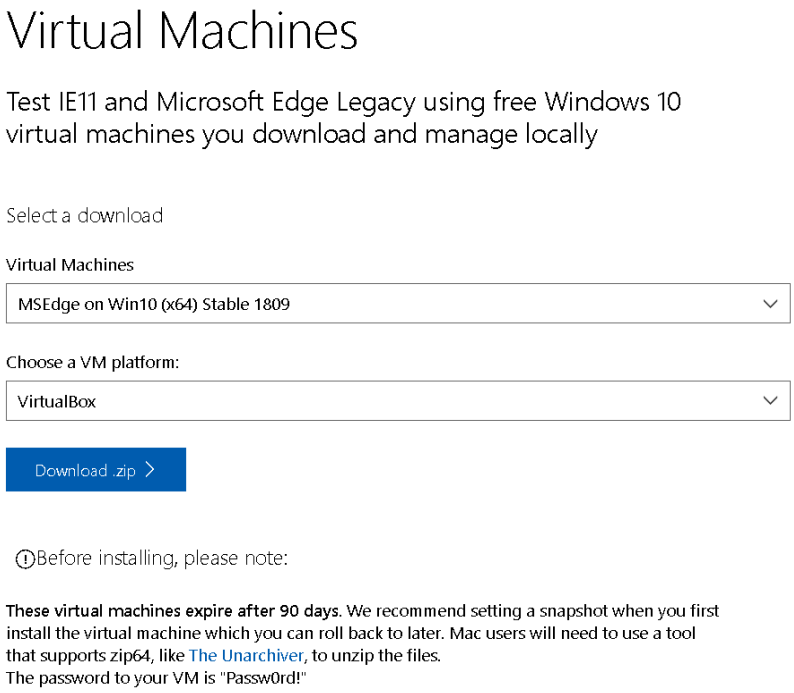
Objectives

- Understand how to use Windows Bitlocker to encrypt the data on the entire volume of a Windows system

Tasks

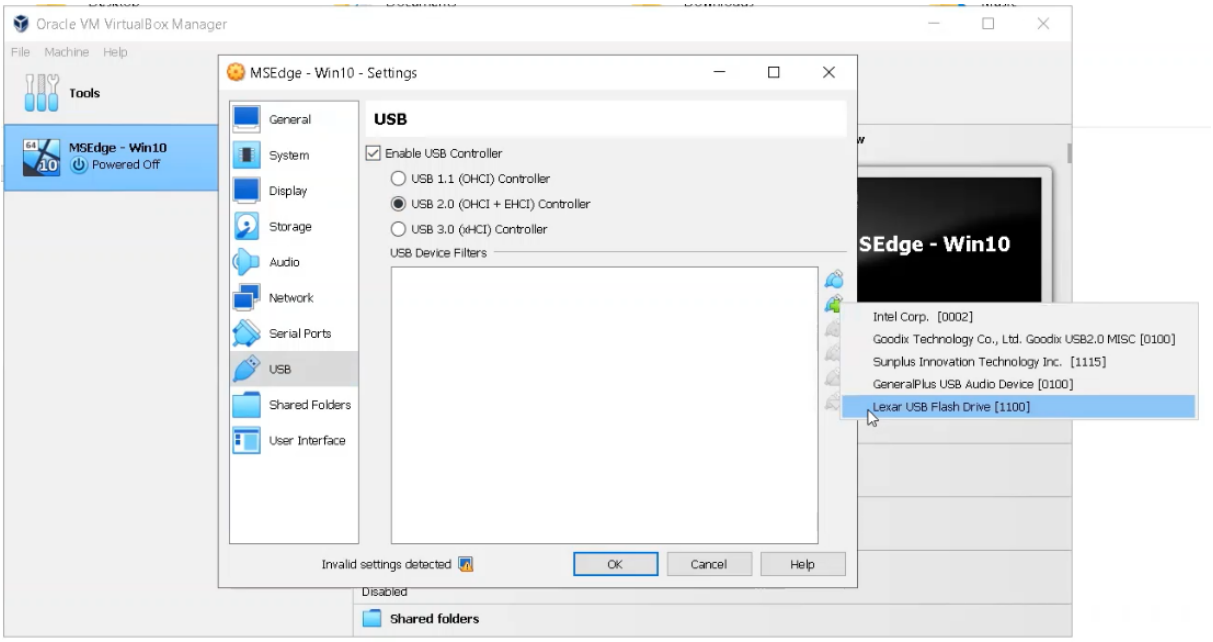
Task 0 (Optional). Prepare a Windows 10 virtual machine

You can download a free premade Windows 10 virtual machine at https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
The virtual machine will expire after 90 days. The password is Passw0rd!
You can choose whichever VM platform you would like. The screenshots in this document will be using VirtualBox.



Task 1. Prepare your USB

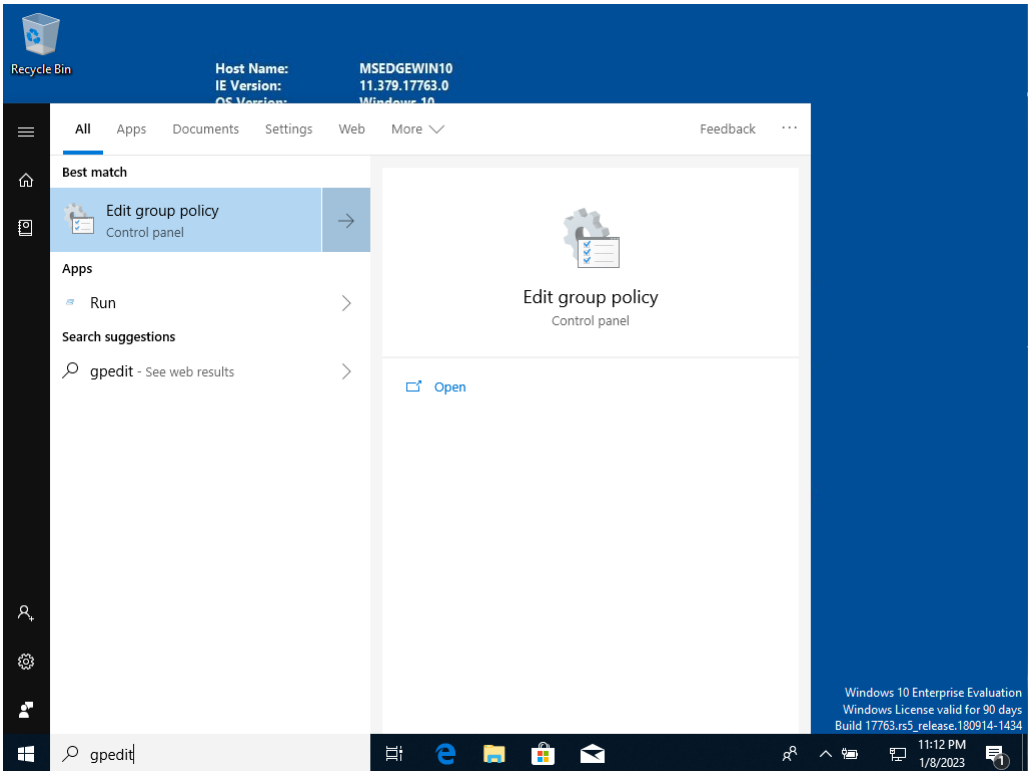
1. Plug in your USB
2. In VirtualBox, click Settings, then navigate to USB and select “Enable USB Controller” and “USB 2.0”. Then click the plug icon with the green plus to add the USB you just plugged in.



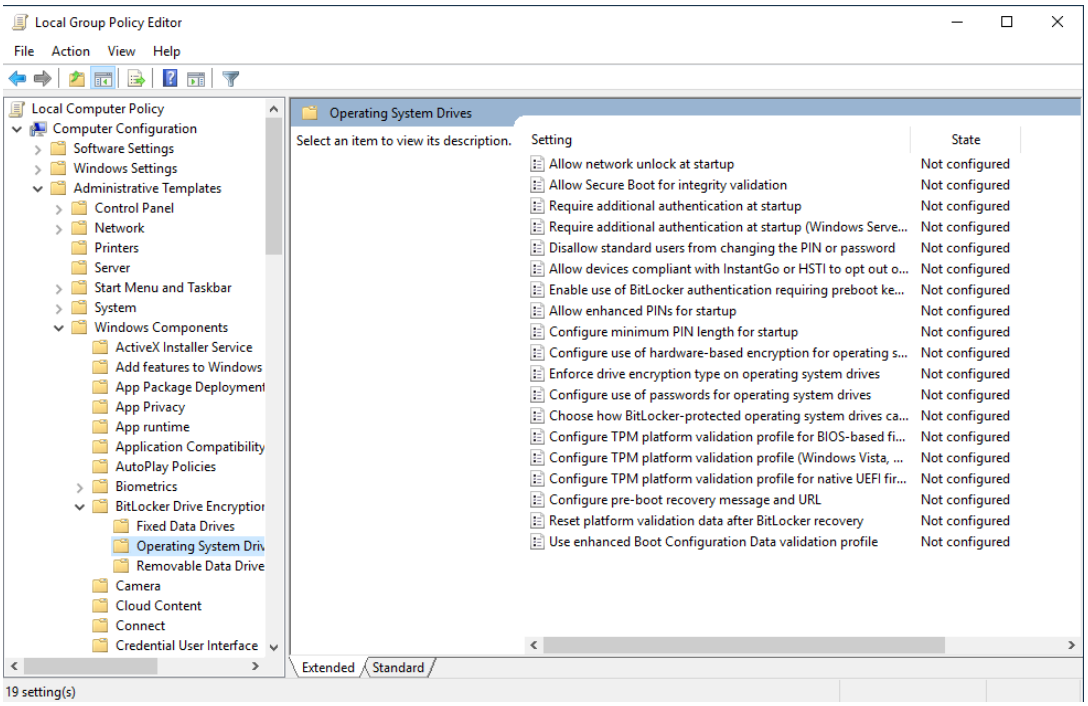
3. When you are done, click OK. Now your USB will automatically eject from your host machine and connect to your virtual machine whenever you start your virtual machine.

Task 2. Enable bitlocker without a compatible TPM

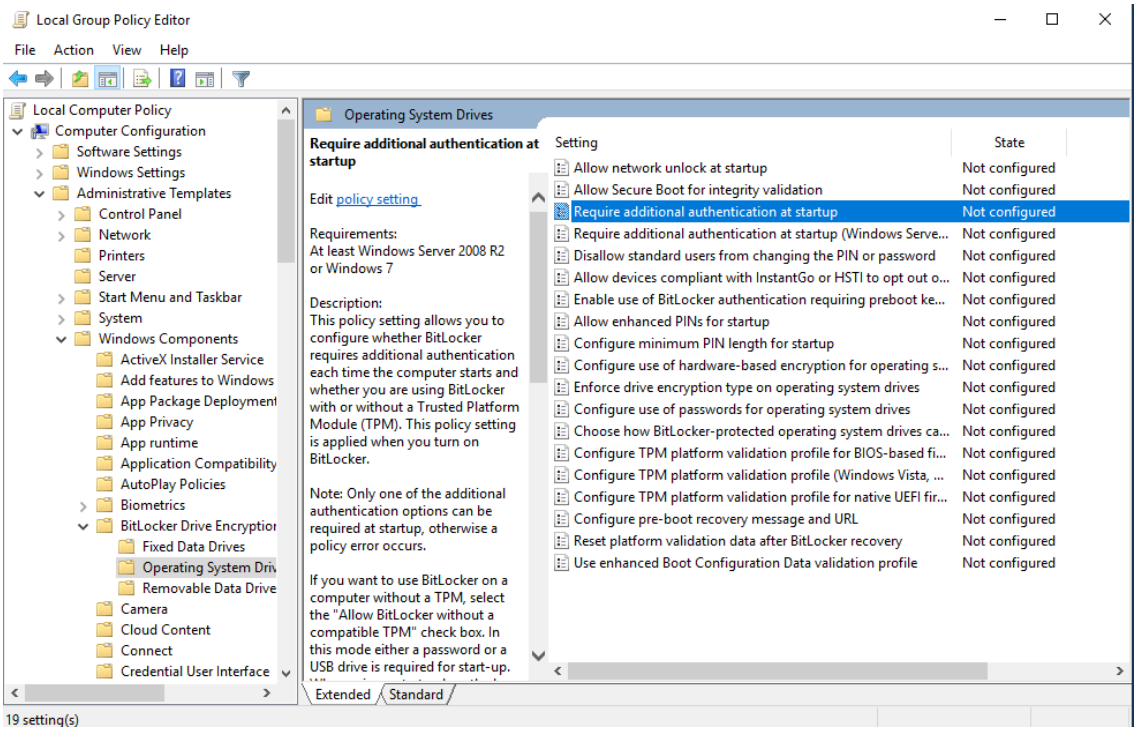
1. In the menu, type “gpedit” and click “Edit group policy”



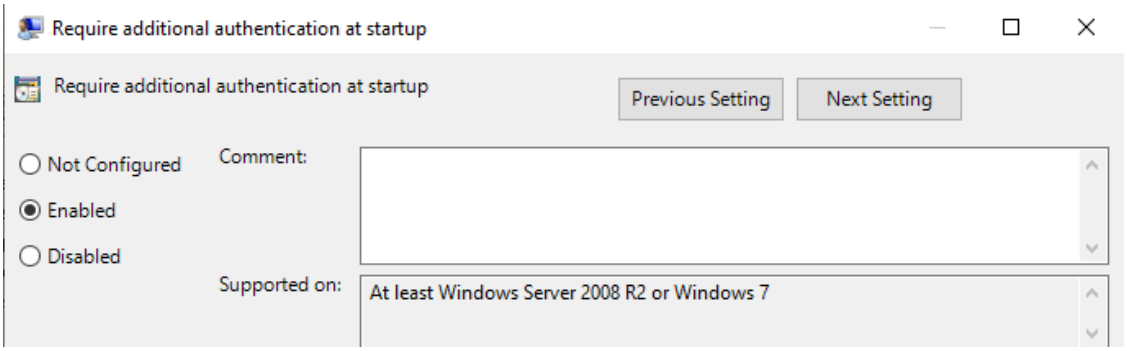
2. Navigate to Computer Configuration > Administrative Templates > Windows Components > Bitlocker Drive Encryption > Fixed Data Drives > Operating System Drives



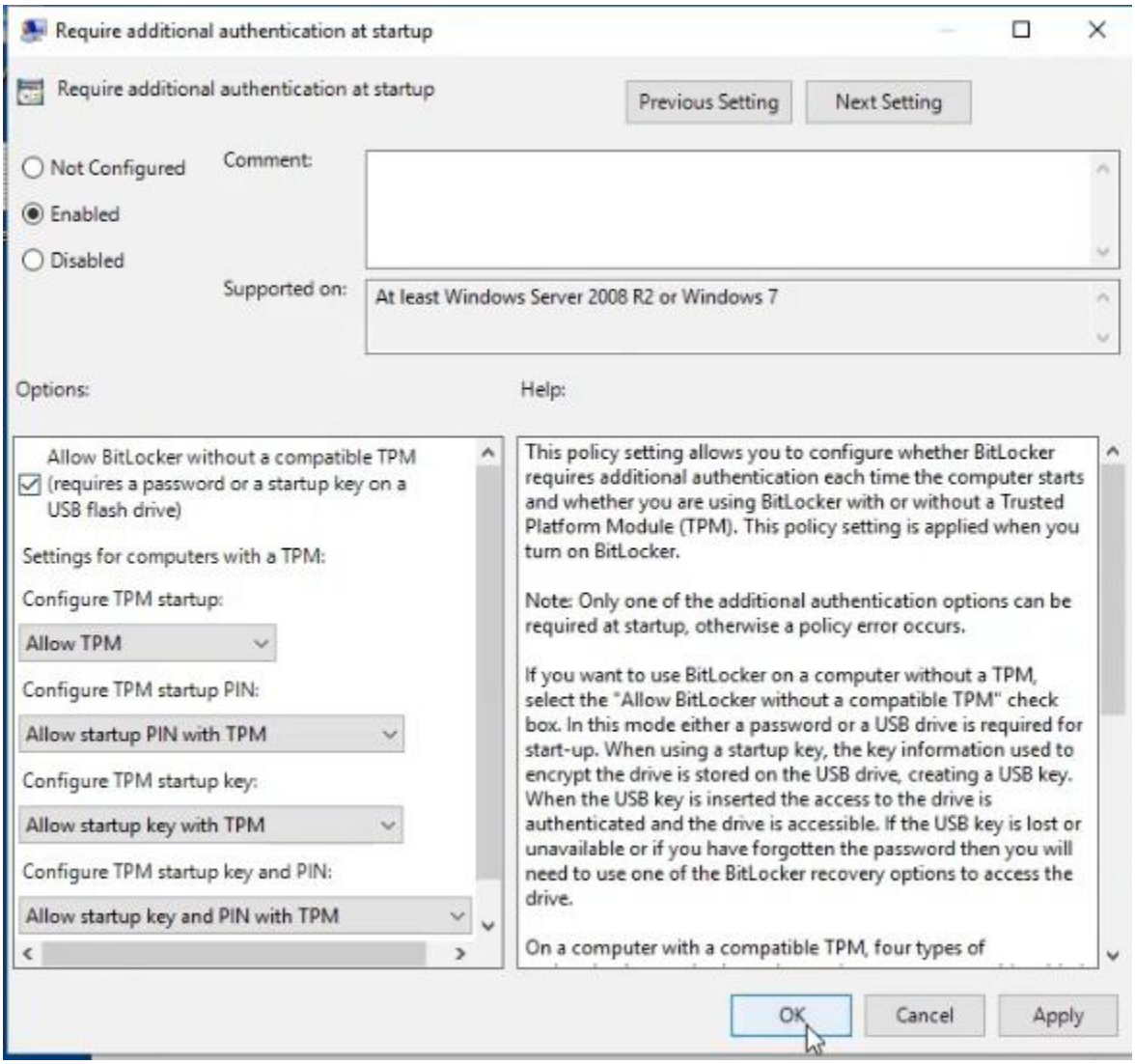
3. Double click “Require additional authentication at startup”



4. Select “Enabled” on the top left



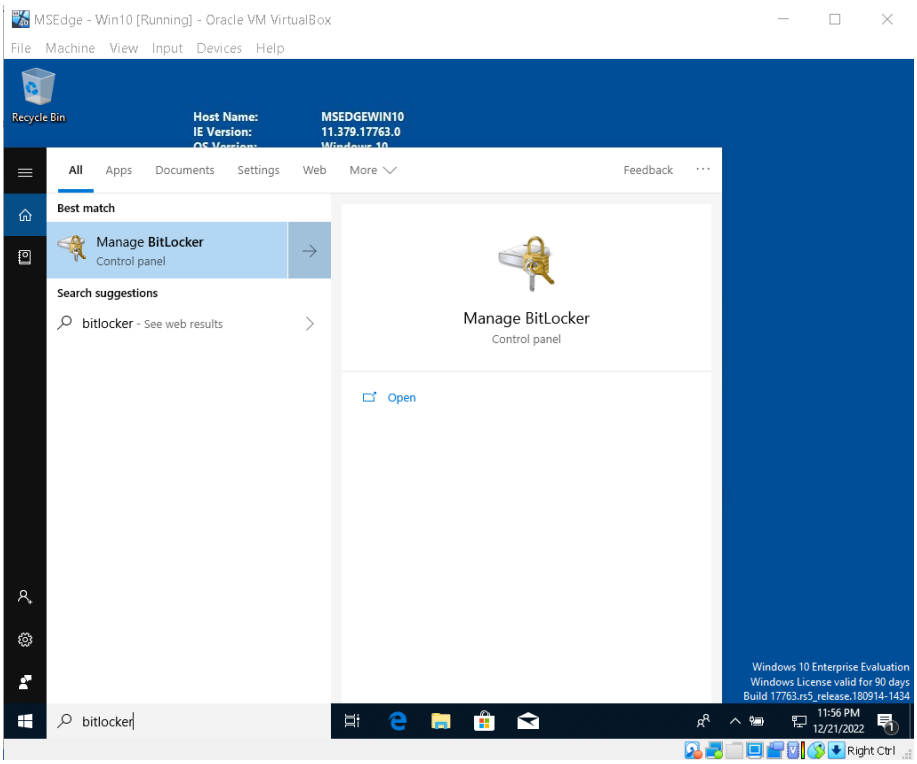
5. Click “OK” on the bottom right when you are done.



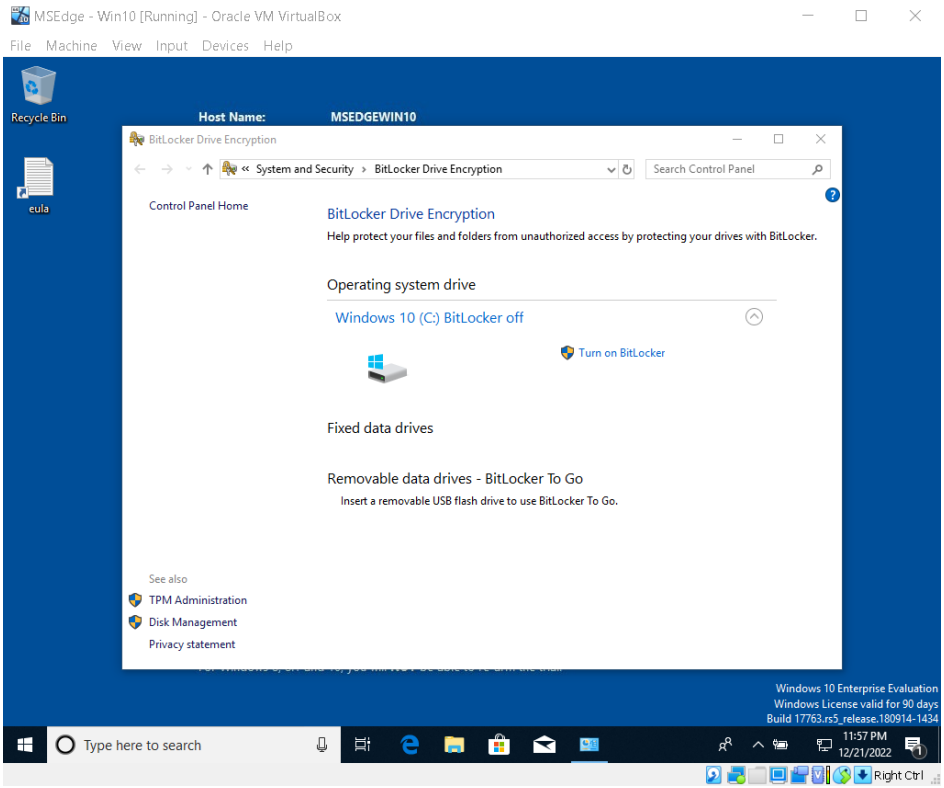
Task 3. Open Windows Bitlocker

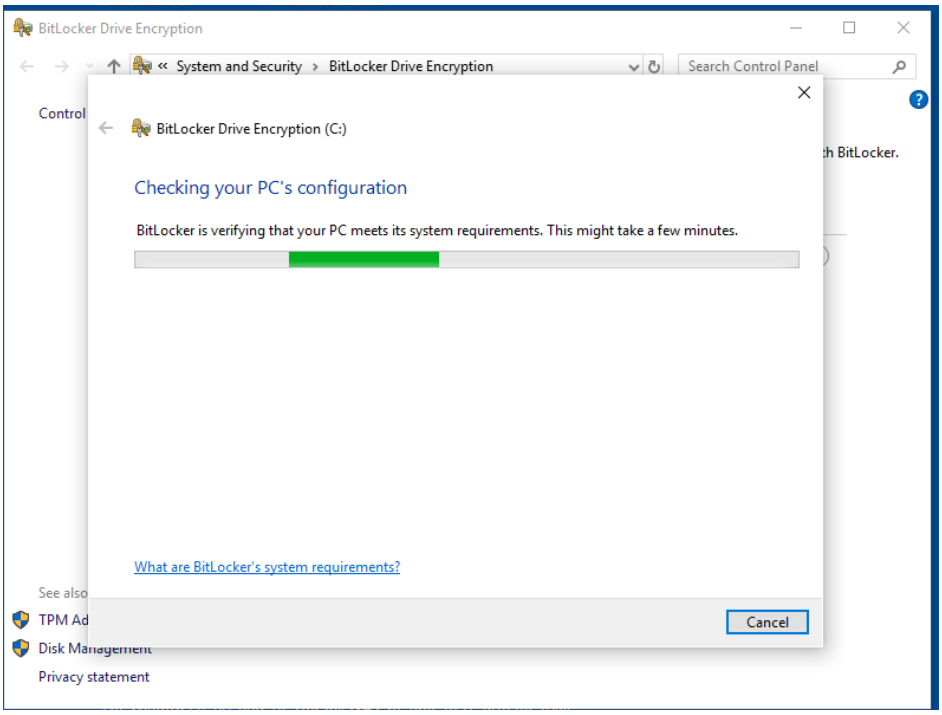
1. Click the menu button on the bottom left of the screen and type “bitlocker”.

Then click “manage bitlocker”

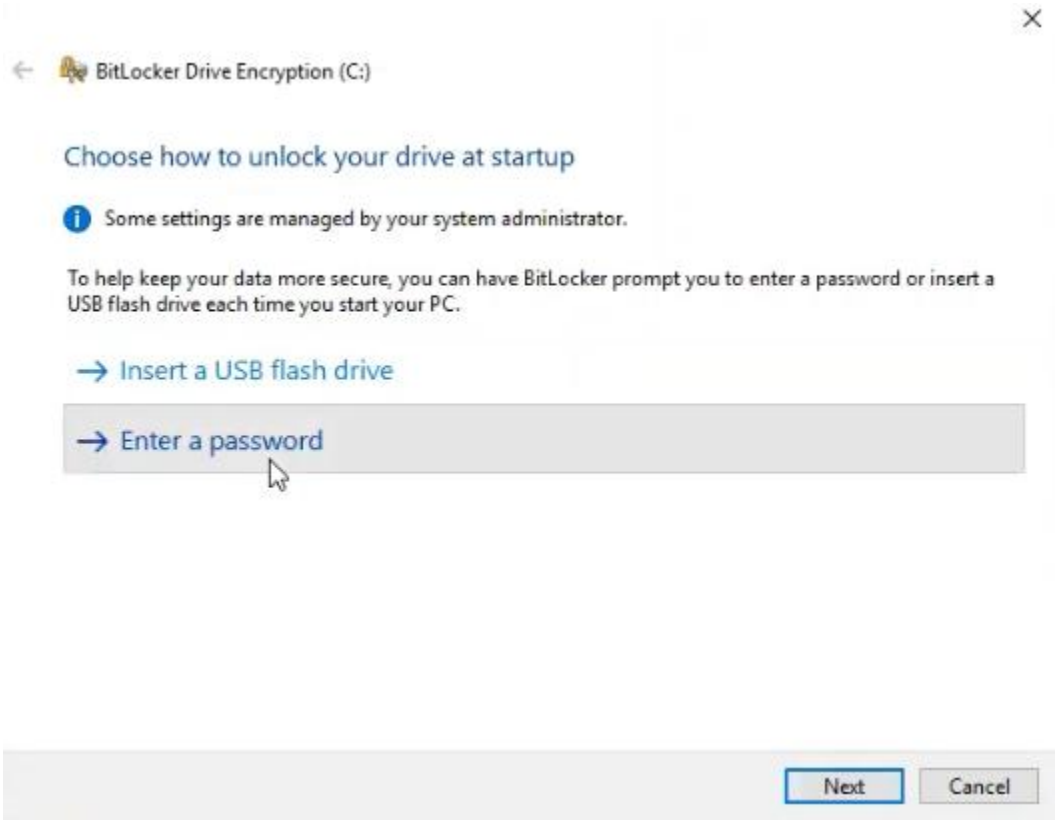


2. Click “Turn on bitlocker”

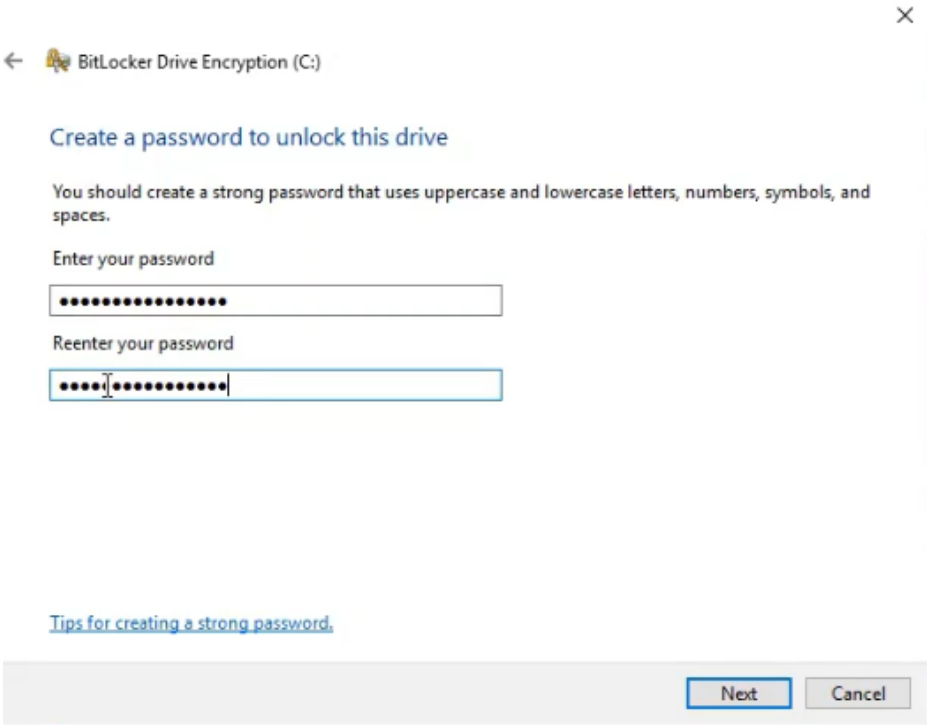




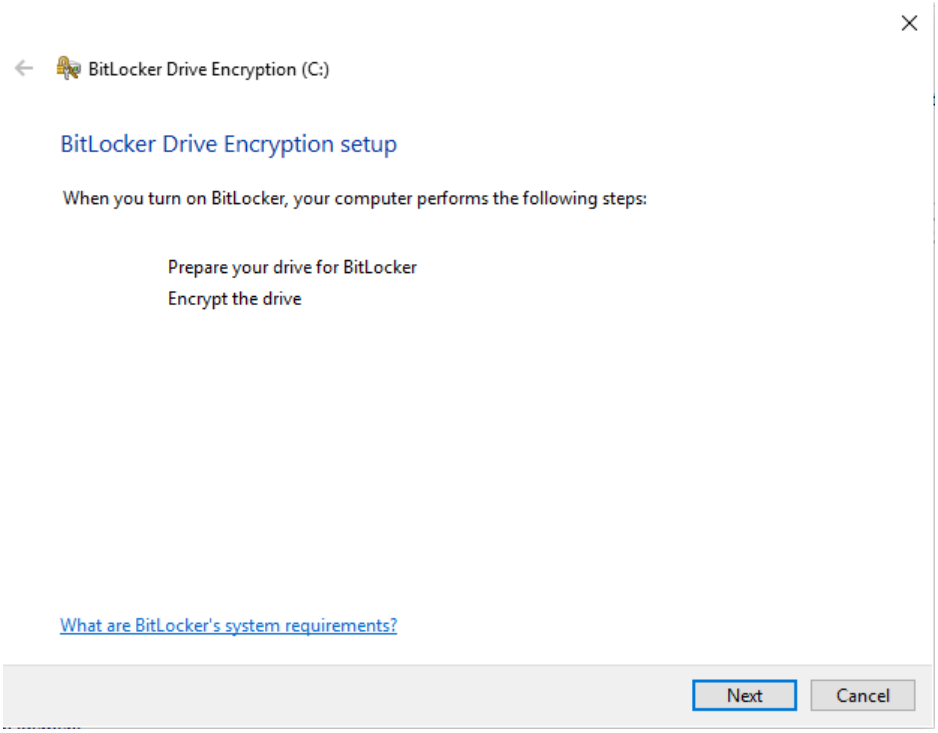
3. Click “Enter a password” then click “Next”



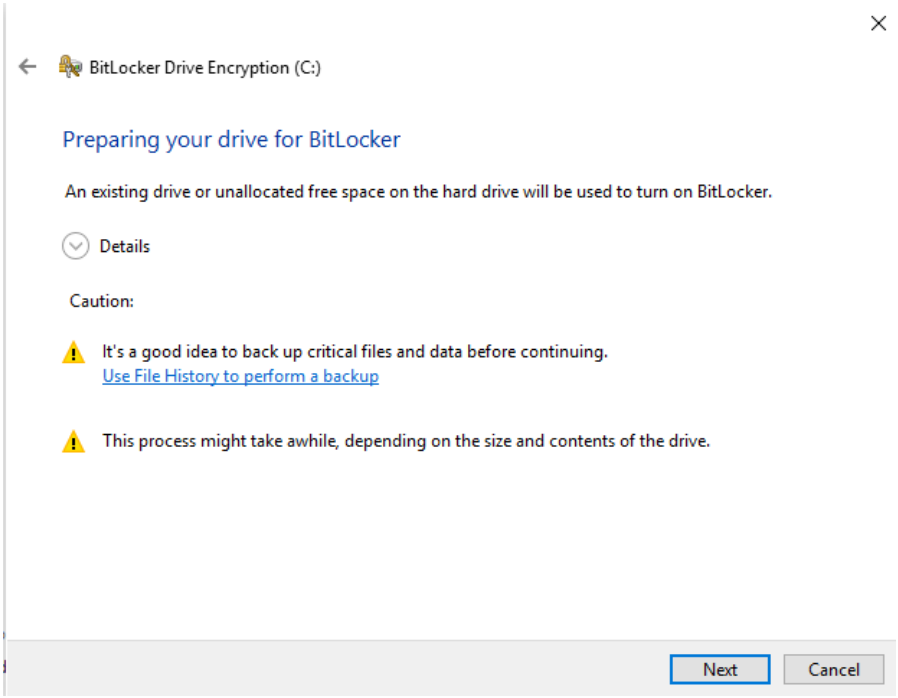
4. Enter any password you want then click “Next”



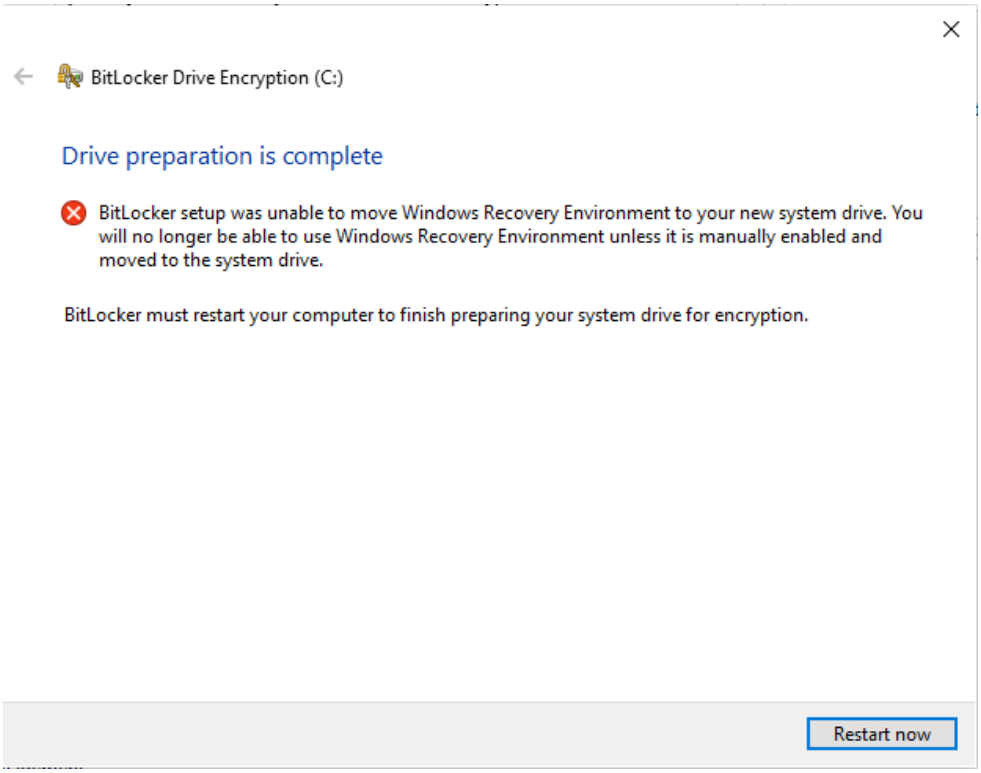
5. Click “Next”



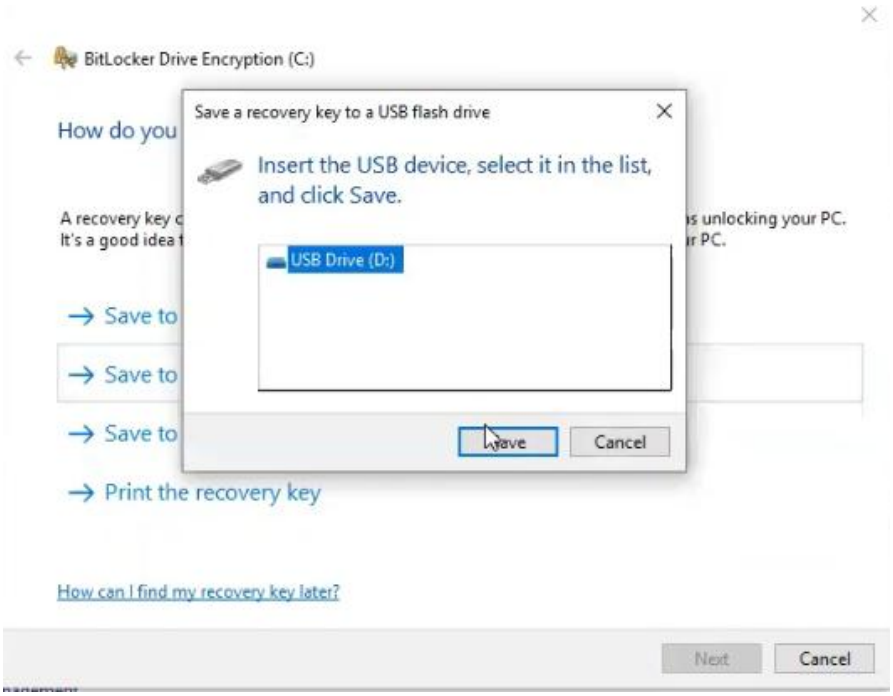
6. Click “Next”



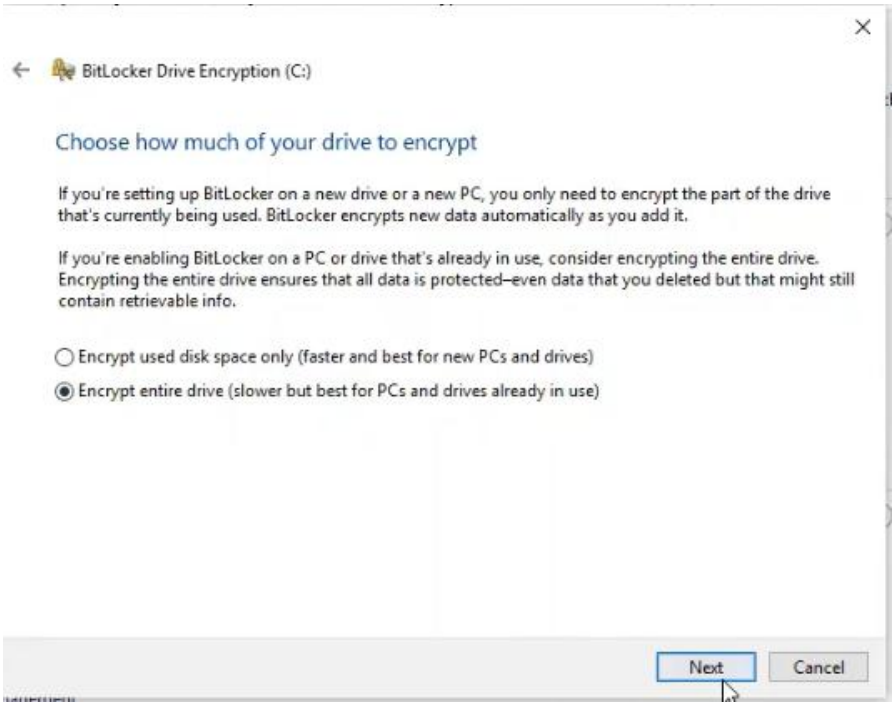
7. Click “Restart now”



8. It will now ask how you want to back up your recovery key. Click “Save to a USB flash drive”. You could also click “save to a file” and navigate to your USB.

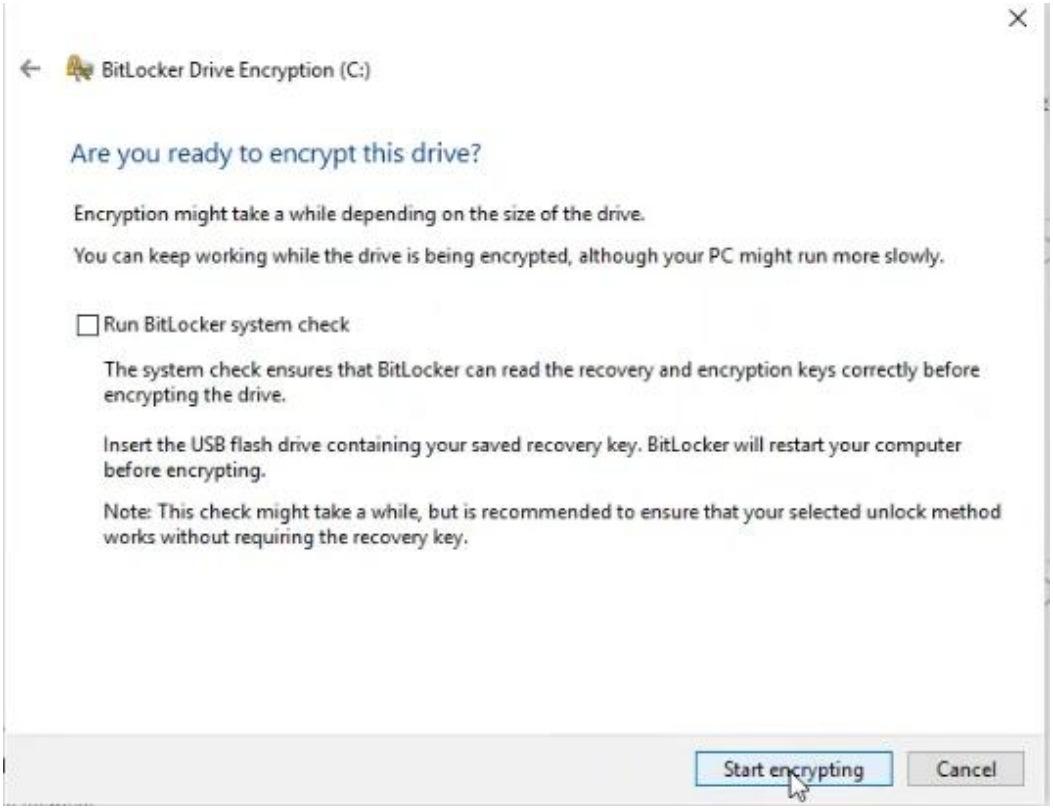


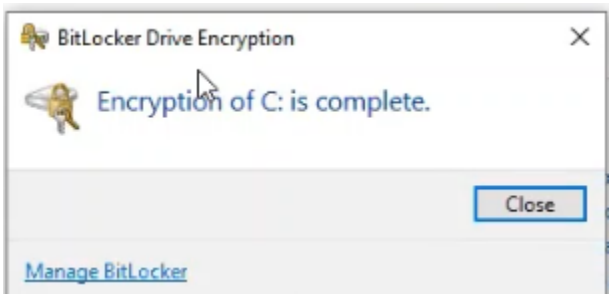
9. Click “Encrypt entire drive” then click “Next”



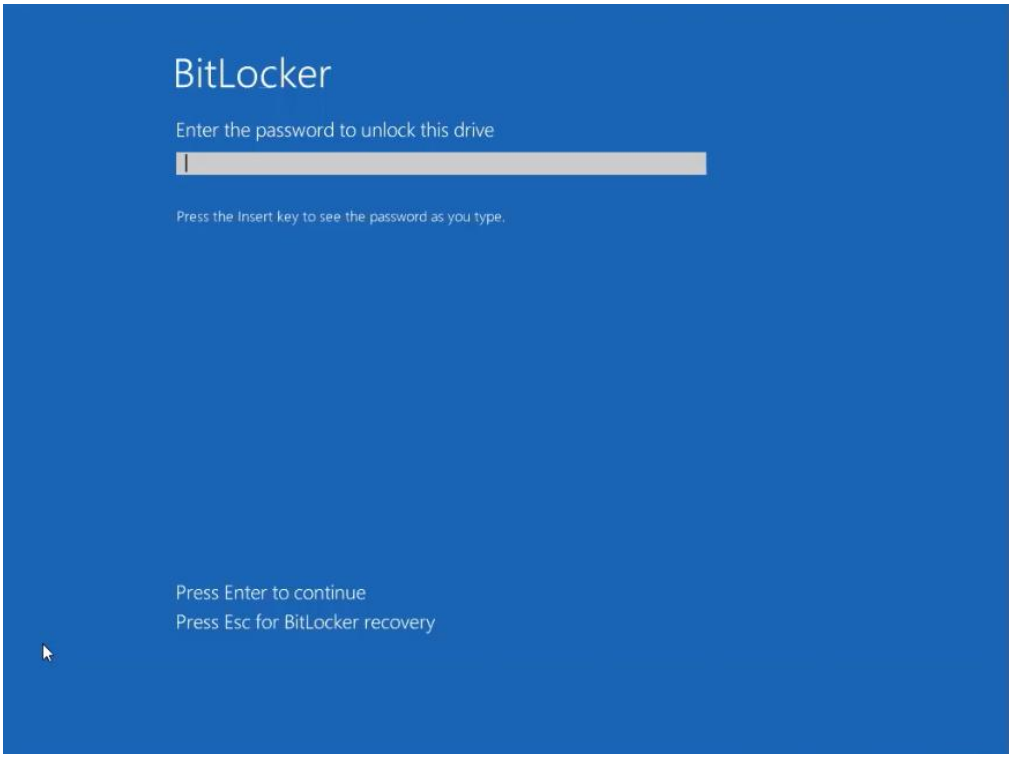
10. Select “New encryption mode” and then “Next”

11. If you are on a **virtual machine**, uncheck “Run bitlocker system check” and then click “Start Encrypting”. If you are on your **personal host machine**, it is best to keep this option checked as a precaution.





12. Now you can restart your machine and see that Bitlocker has been enabled



Questions:

1. What is required to allow Bitlocker without a compatible TPM?
2. What does running a Bitlocker system check do? Why would this be important?
3. When would you want to encrypt your entire drive?
4. What is another way you can unlock your device if you don’t have the password?
5. Why do you think a USB is needed? What would happen if you saved the recovery key on the drive itself?