# **Exercise 1 - Configuring BitLocker.**

BitLocker is a security technology that encrypts the entire hard drive, protecting both the operating system and user data. Whether the computer is turned on or off, BitLocker's protection is maintained on the encrypted drive. Consequently, this Even against 'offline attacks' by hackers, technology preserves the confidentiality of disk contents. To see the contents on another computer, disable Windows or physically remove the hard disk computer.

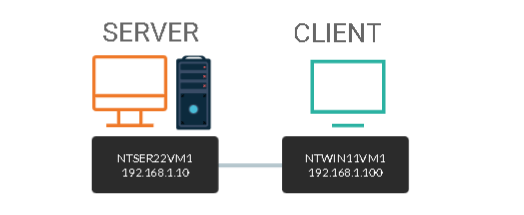
A Trusted Platform Module (TPM) chip is required for BitLocker, which provides integrated protection for Windows and data files during the operating system's boot phase. TPM is a microchip that is embedded on a system motherboard and is enabled via the computer's BIOS.

The hard disk of a Windows 10 computer must have two partitions: a system partition that holds the files for launching Windows and a partition that hosts C:\Windows, which stores the operating system data. To encrypt a disk volume or partition, BitLocker requires the NTFS file system.

In this exercise,

1. Let’s create an additional disk volume considered as a data volume protected with BitLocker.
2. Shrink Volume and Create Secondary Volume
3. Enable Local Group Policy Object for BitLocker
4. Encrypt Data Drive with BitLocker
5. Manage BitLocker-Enabled Drive with Manage-Bde

## **Topology**



DOMAIN = networktute.com

NTSER22VM1 = Windows Server 2022 – Domain Controller

NTWIN11VM1 = Windows 11 – Domain Member

## **Prerequisite**

* *VMware Workstation 16 Pro*
  + When making this tutorial, we used the “Windows Server 2019” VM Template and “Windows 10 & later” VM Template. Since VMware didn’t have the updated templates.
* *Microsoft Windows Server 2022*
* *Microsoft Windows 11*

## **Task 1: Configure Disk Cleanup**

The encryption of the disk volume where Windows is installed is supported by BitLocker. Due to this constraint, you will not be able to see the BitLocker password question during the pre-login step in this experiment.

In this task, we will shrink the primary hard disk and use the reclaimed disk space as a secondary volume. The secondary disk volume will be protected with BitLocker.

**Step 1:**

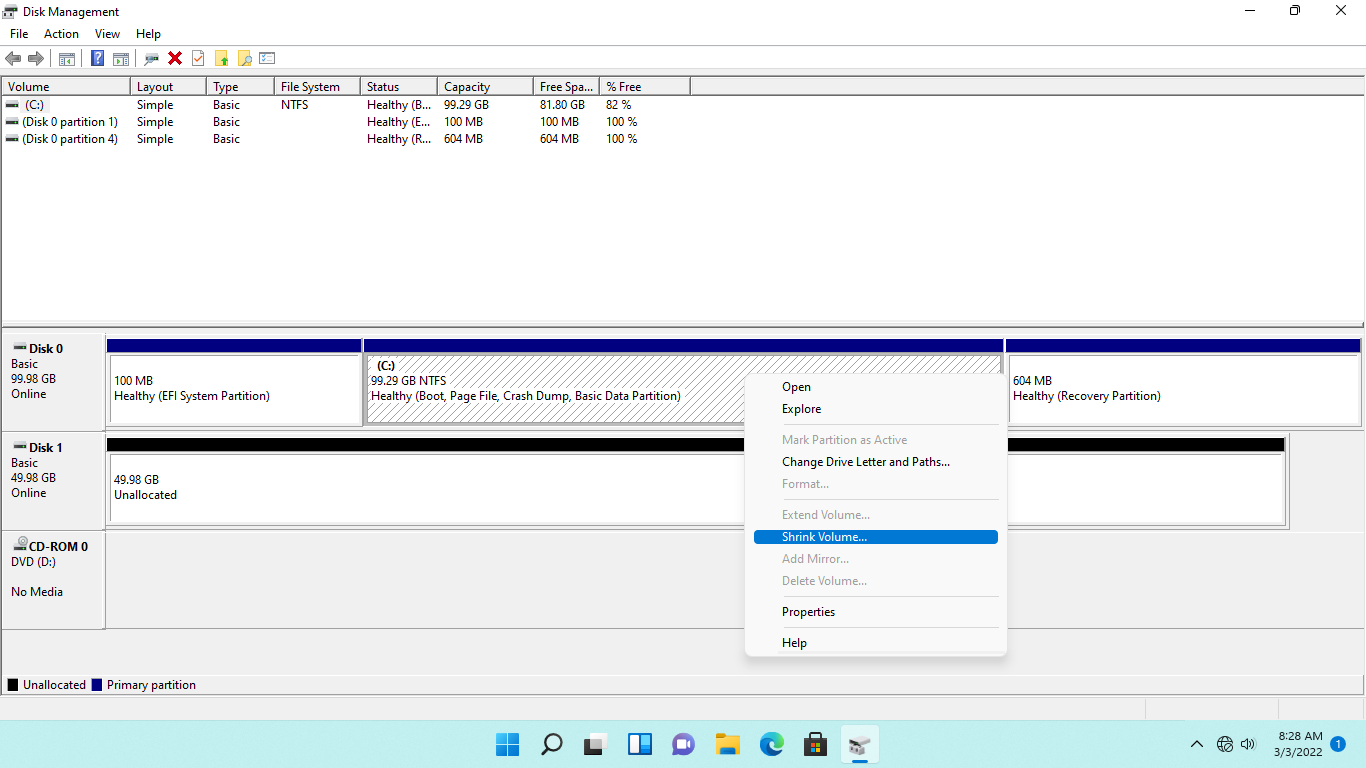
Make sure you have powered on the devices and connect to **NTWIN11VM1**.

Right-click the Start icon and select **Disk Management**.

If the **Initialize Disk** dialog box appears, click **OK**.

On the **Disk Management** window, right-click **Disk (C:)** and select **Shrink Volume**

|  |
| --- |
| If you still see volumes from a prior task, right-click on each one and choose Delete Volume... to free up space. |

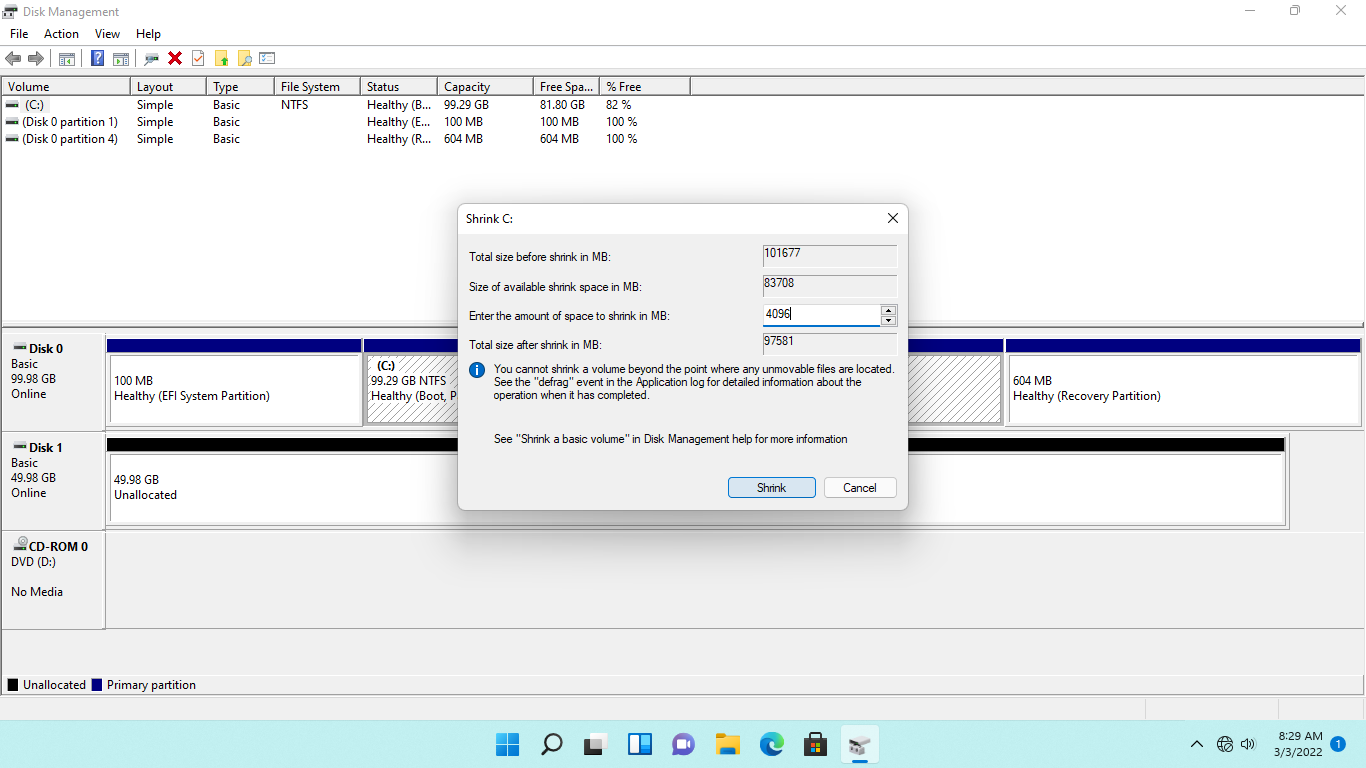


**Step 2:**

Please wait while Disk Management queries the storage.

On the **Shrink C**: dialog box, type-over the value in the **Enter the amount of disk space to shrink in MB** with the following: ***4096***

Click **Shrink**.

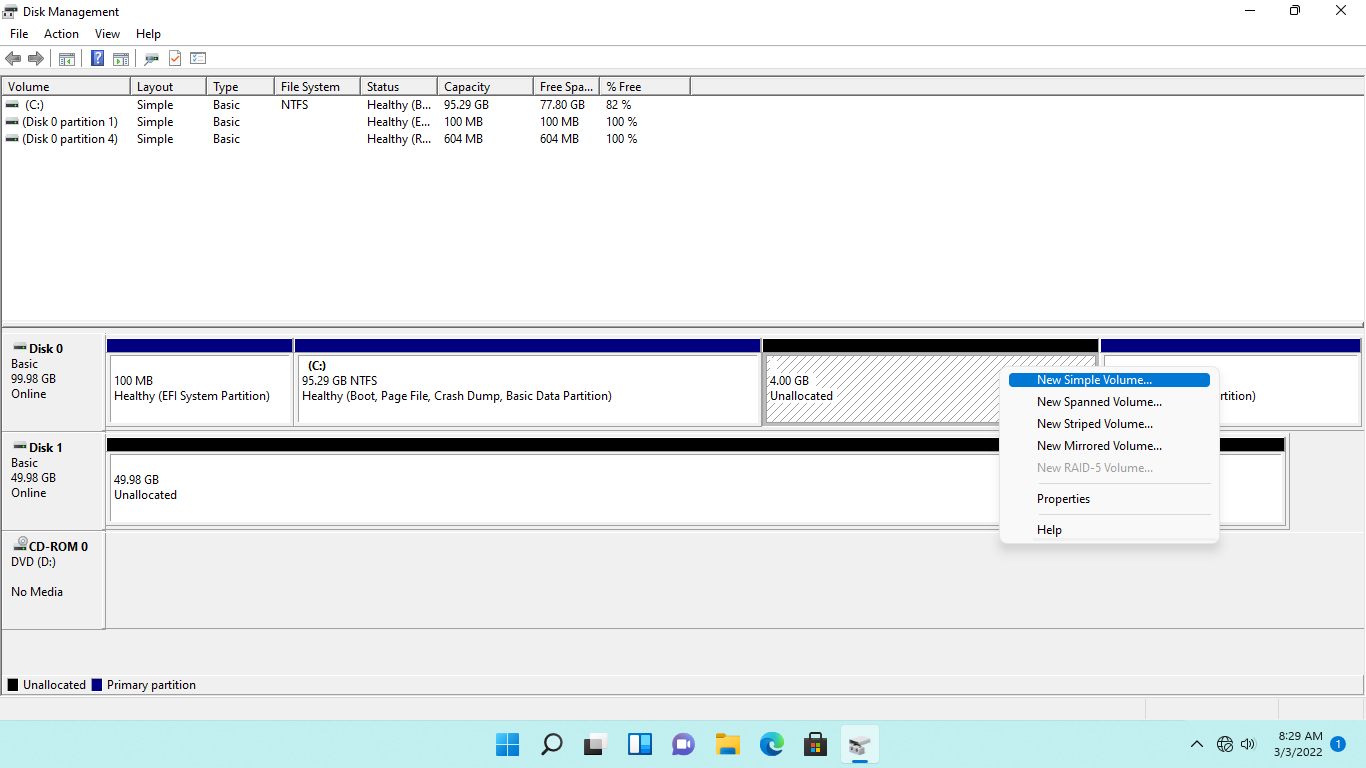


**Step 3:**

Please wait while **Disk Management** shrinks the volume.

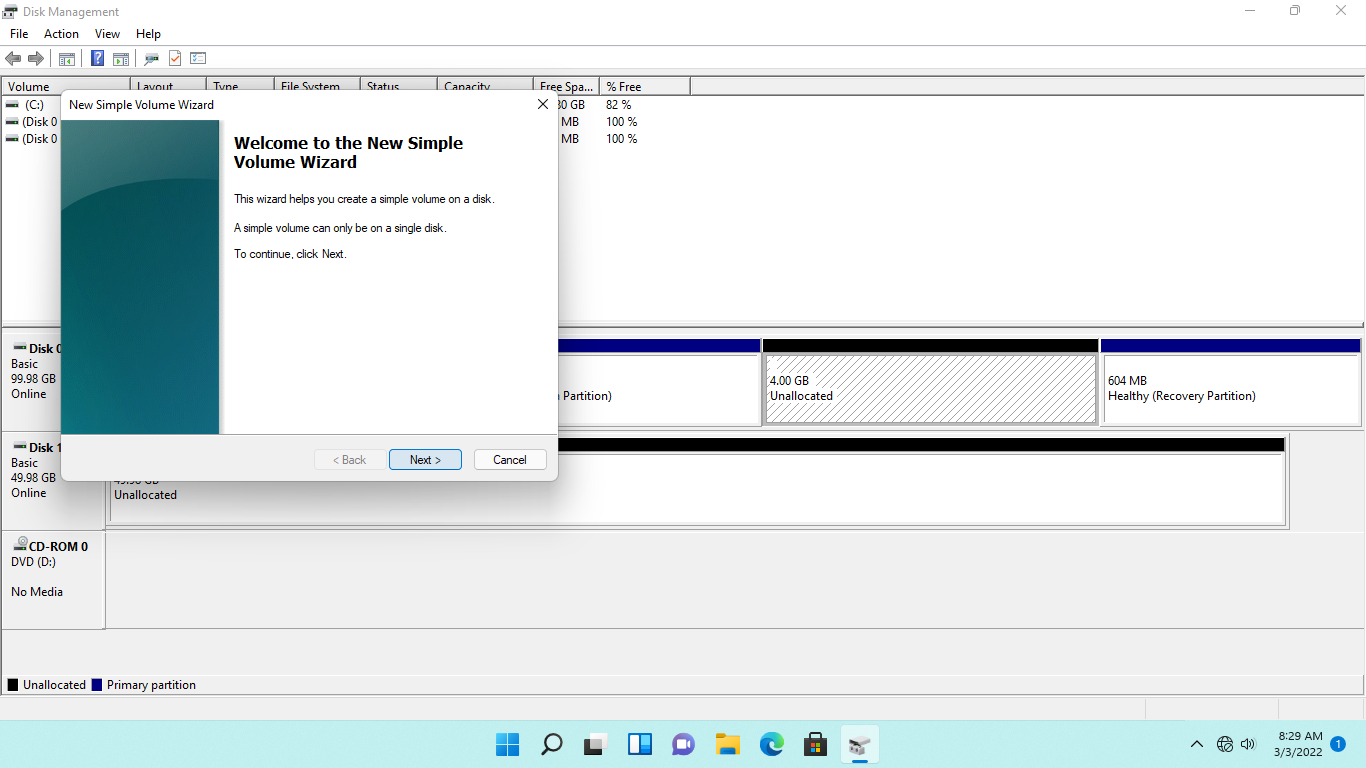
Notice that the status of **Disk 0** now has a **4.00 GB Unallocated** partition.

On **Disk 0**, right-click the **Unallocated** partition and select **New Simple Volume.**



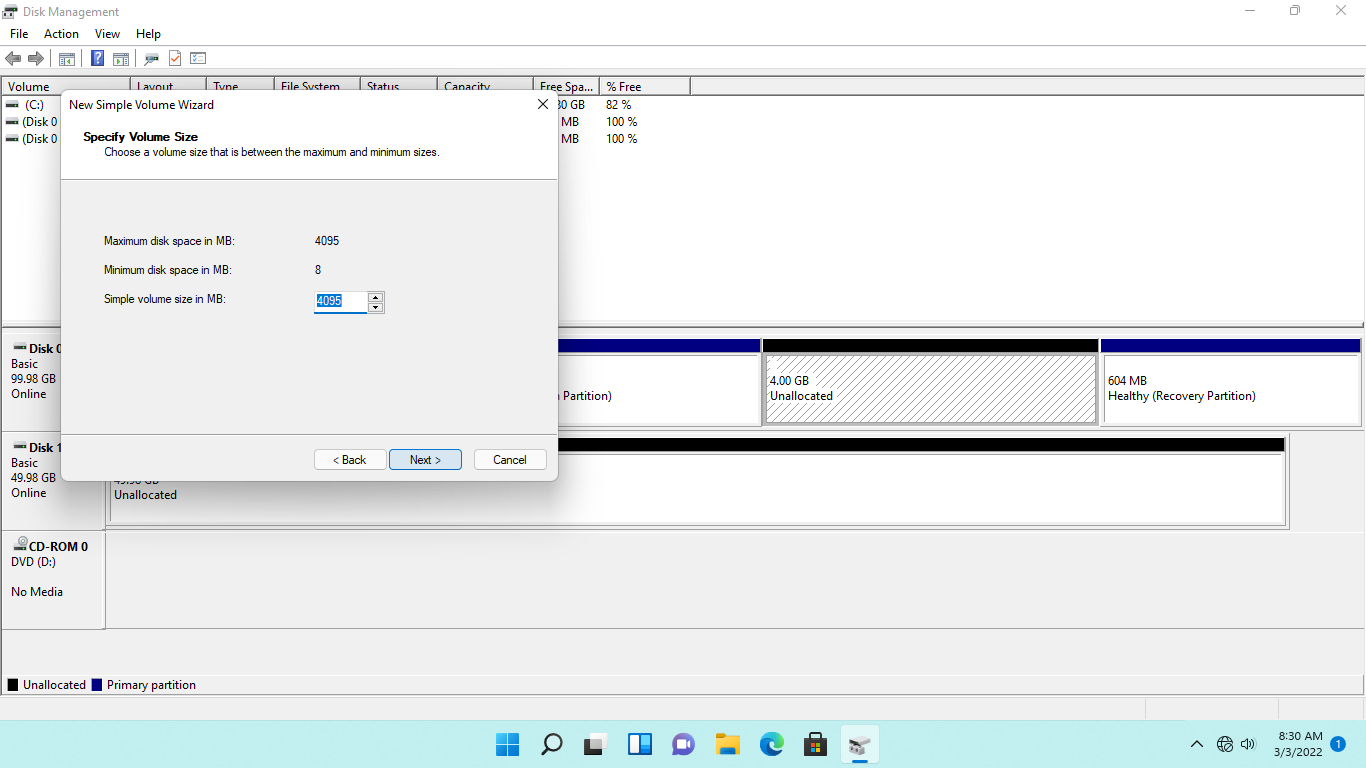
**Step 4:**

On the **New Simple Volume Wizard - Welcome to the New Simple Volume Wizard** page, read the information and click **Next**



**Step 5:**

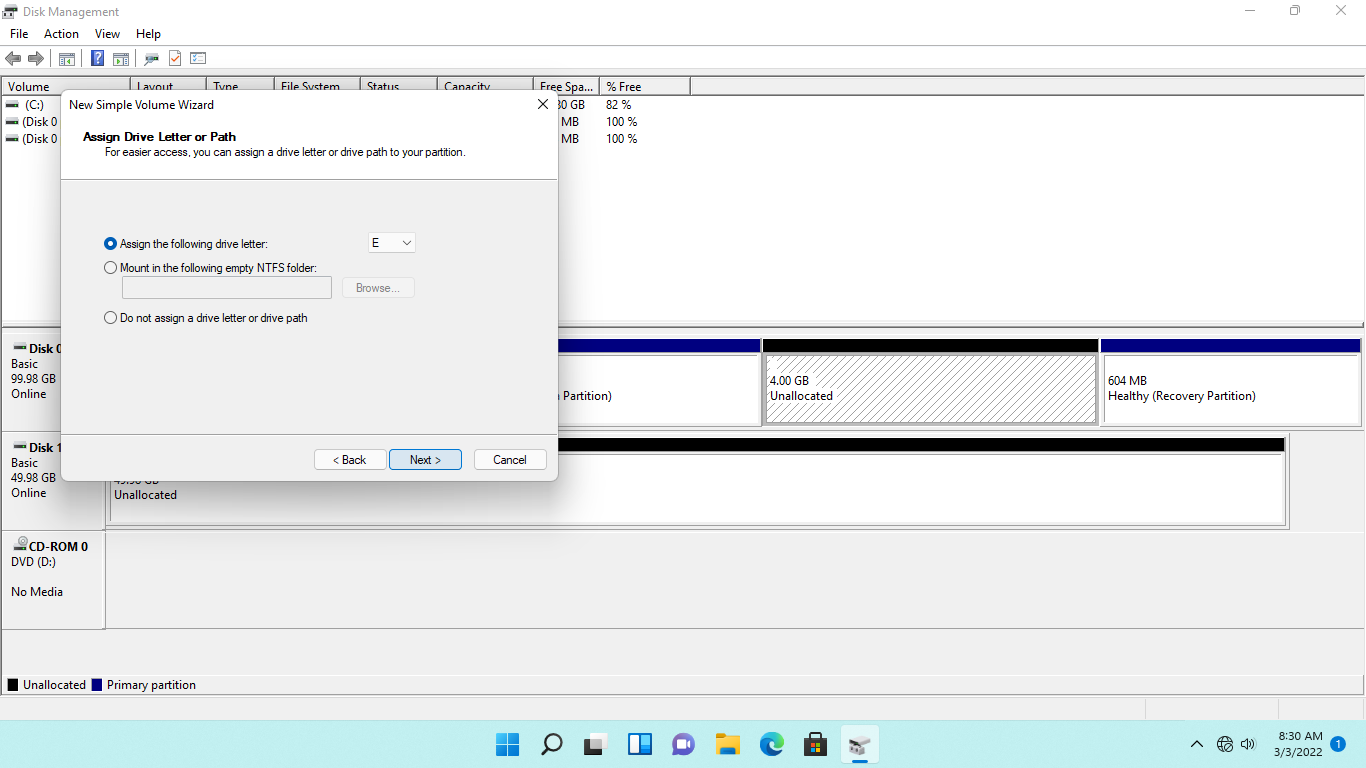
On the **Specify Volume Size** page, accept the default settings and click **Next**.



**Step 6:**

On the **Assign Drive Letter or Path** page, keep the default specifications.

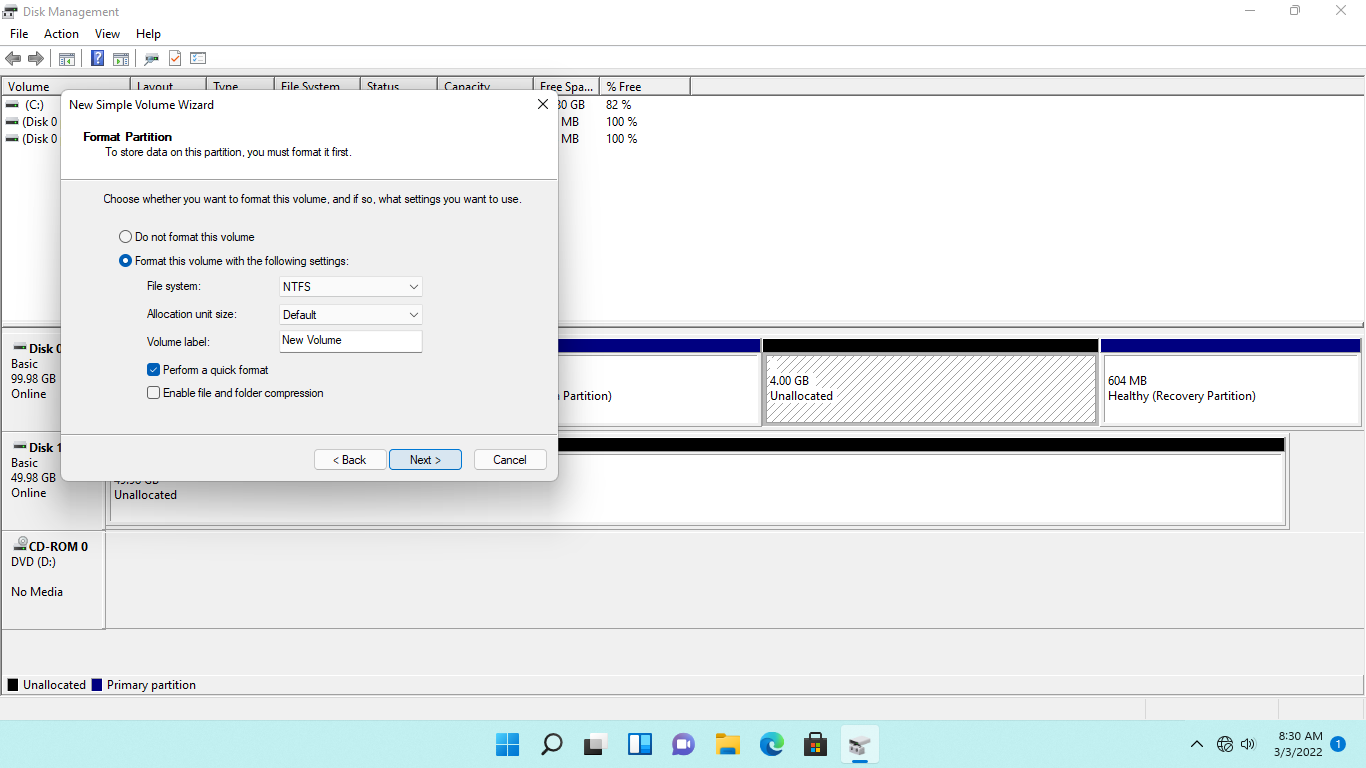
Click **Next.**



**Step 7:**

On the **Format Partition** page, keep the default settings.

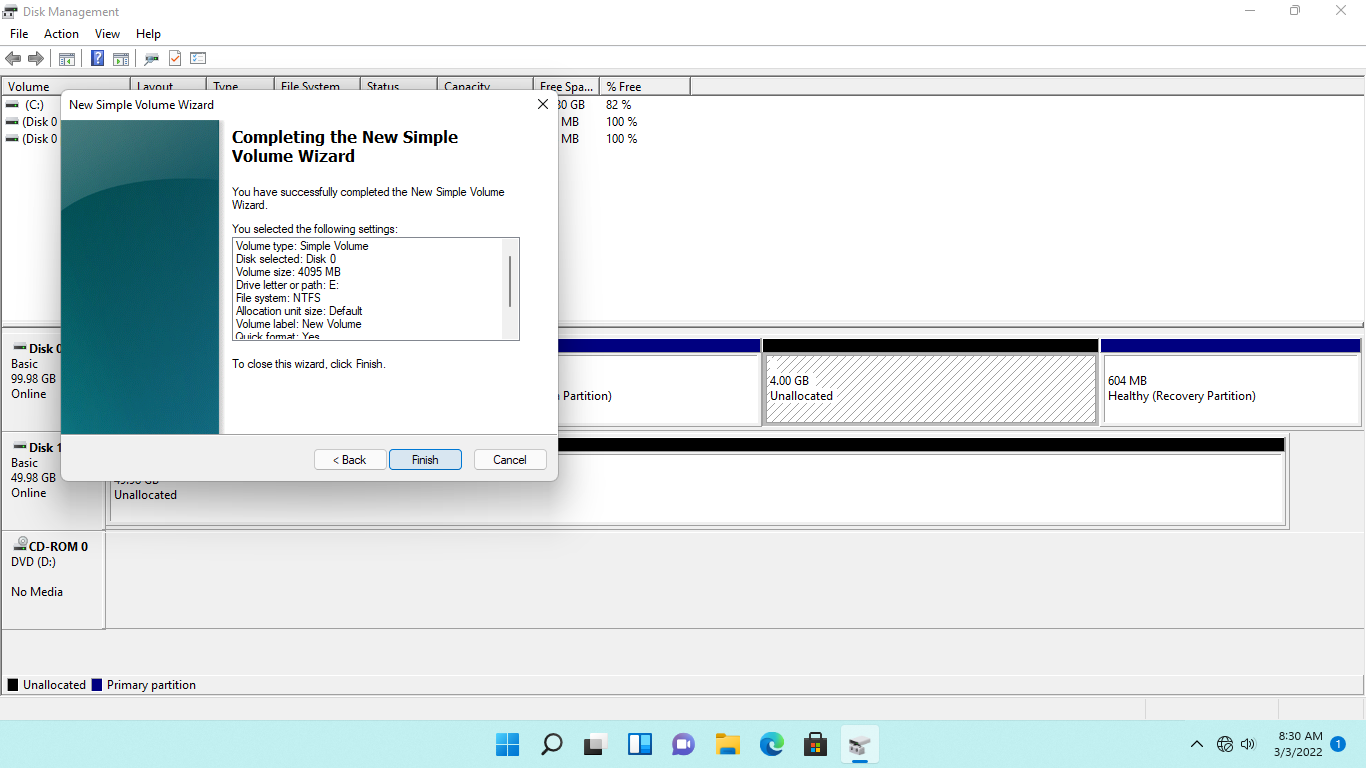
Click **Next.**



**Step 8:**

On the **Completing the New Simple Volume Wizard** page, read through the summary about this new disk volume.

Click **Finish** to create the specified volume and exit the wizard.

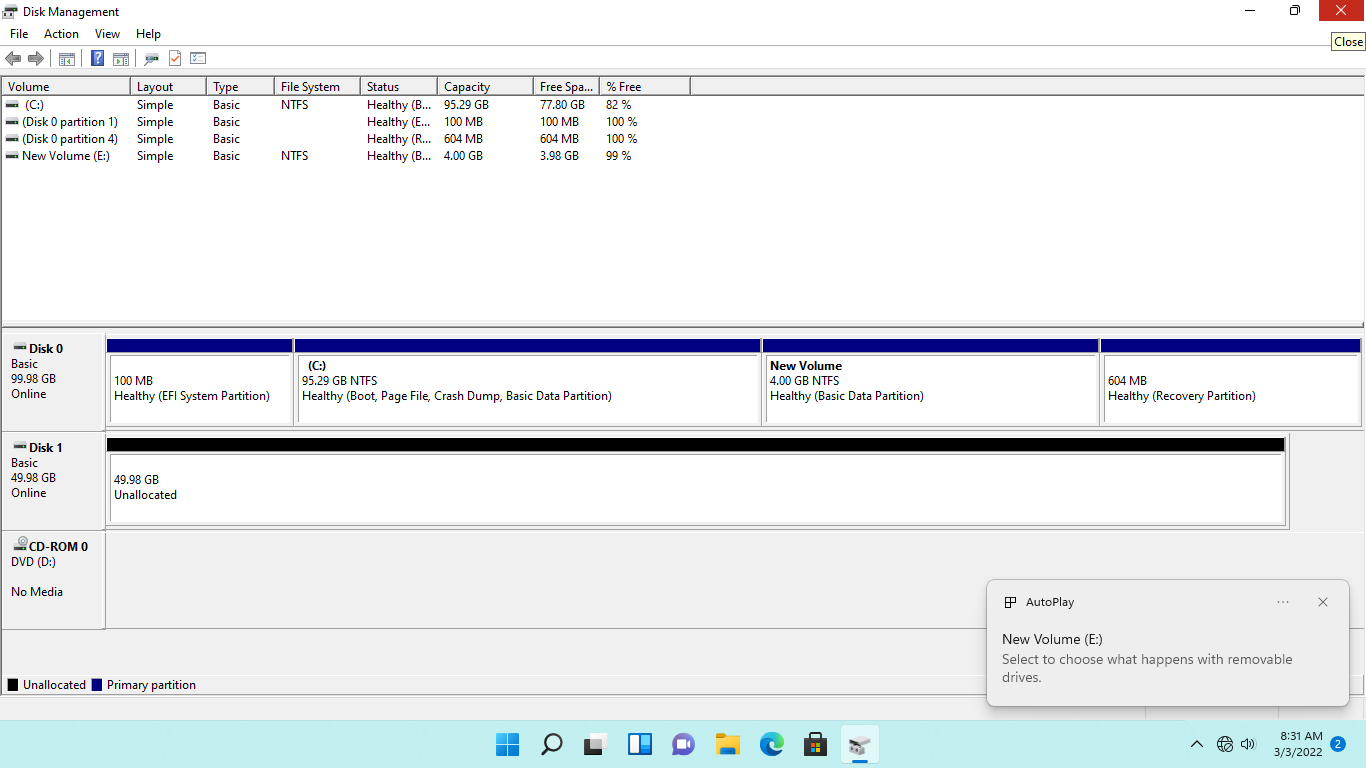


**Step 9:**

If asked if you want to format the newly-created disk volume, click **Cancel** to dismiss the prompt. This may appear as a minimized icon on the **Taskbar**.

Back on the **Disk Mana**gement window, notice that **New Volume (E:)** is now available.

Close the **Disk Management** window.



## **Task 2: Enable Local Group Policy Object for BitLocker**

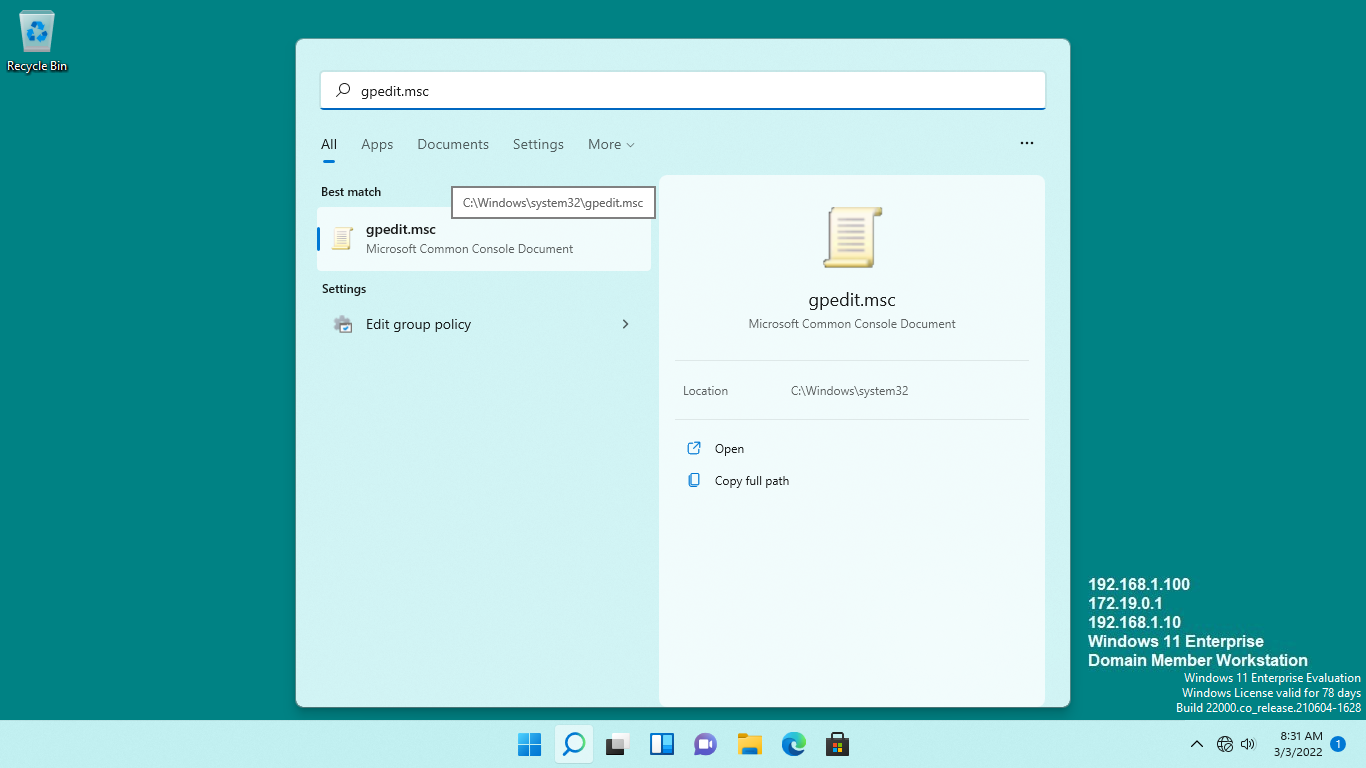
If a Trusted Platform Module (TPM) chip is not supported on a Windows device, such as this lab, use a group policy object to activate BitLocker on the Windows PC without a TPM chip.

In this task, we will enable a group policy setting to bypass the detection of a TPM chip on Windows.

**Step 1:**

On the **NTWIN11VM1** desktop, click in the Type here to search textbox and type: ***gpedit.msc***

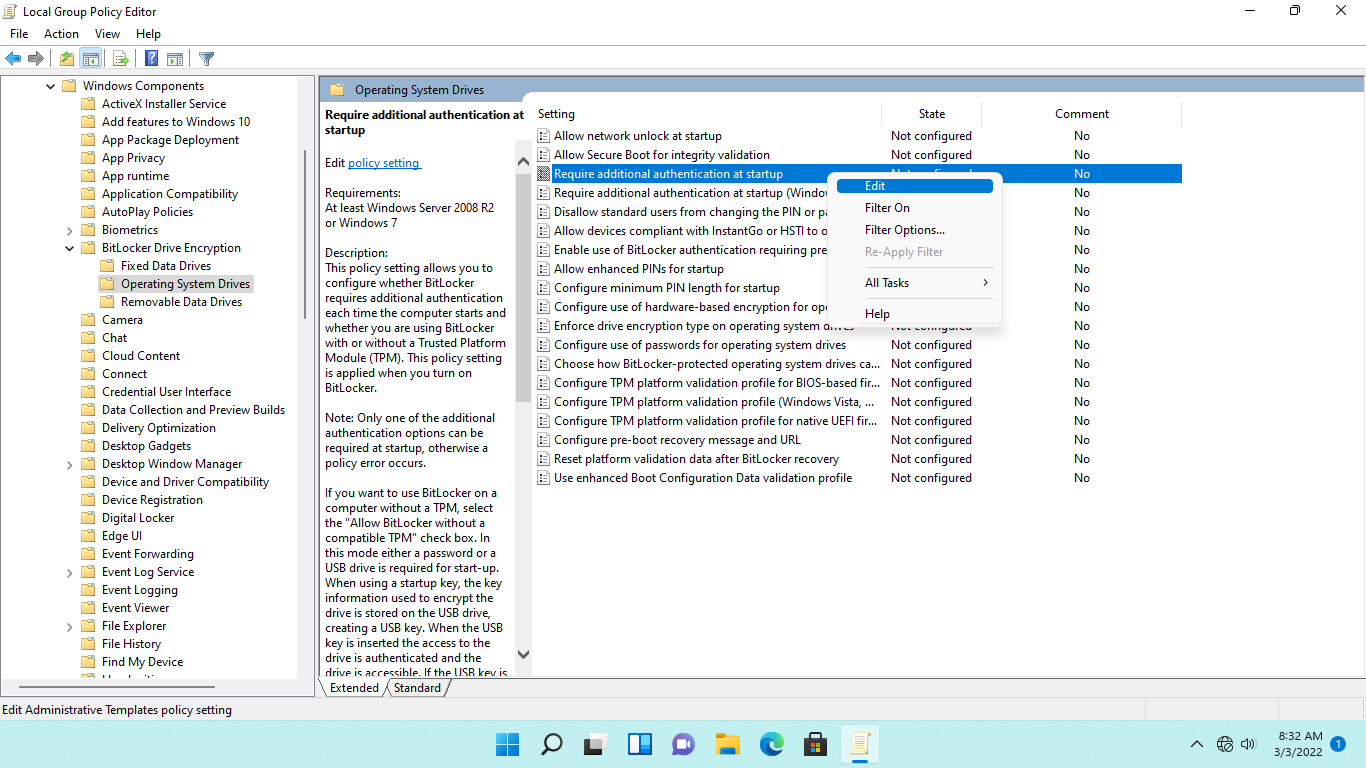
Press **Enter** or select **Edit group policy** from the menu.



**Step 2:**

On the **Local Group Policy Editor** window, expand **Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption** and then click the **Operating System Drives** folder.

Go to the details pane, right-click the **Require additional authentication** at startup setting and select **Edit**.



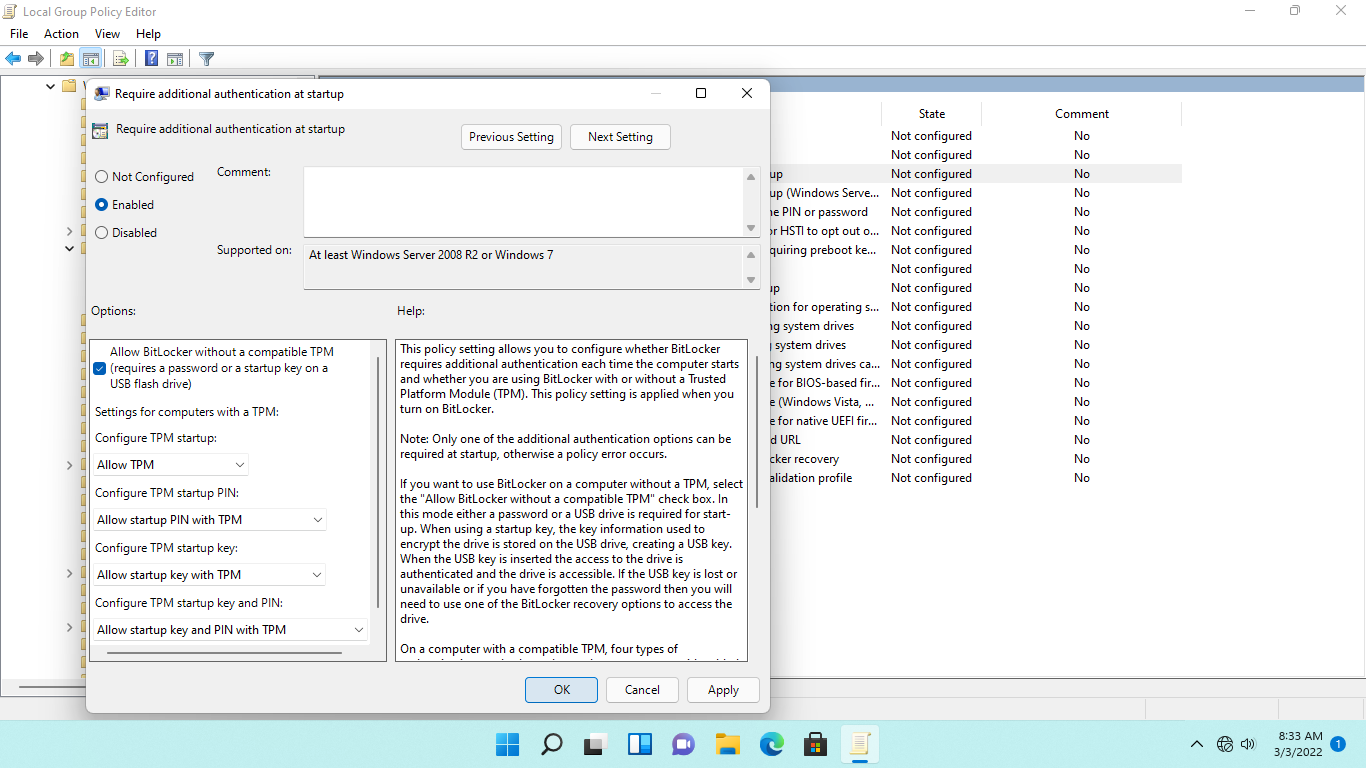
**Step 3:**

On the **Require additional authentication at startup** dialog box, select the **Enabled** radio button.

Further down the **Options** section, ensure that the **Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)** checkbox is ticked.

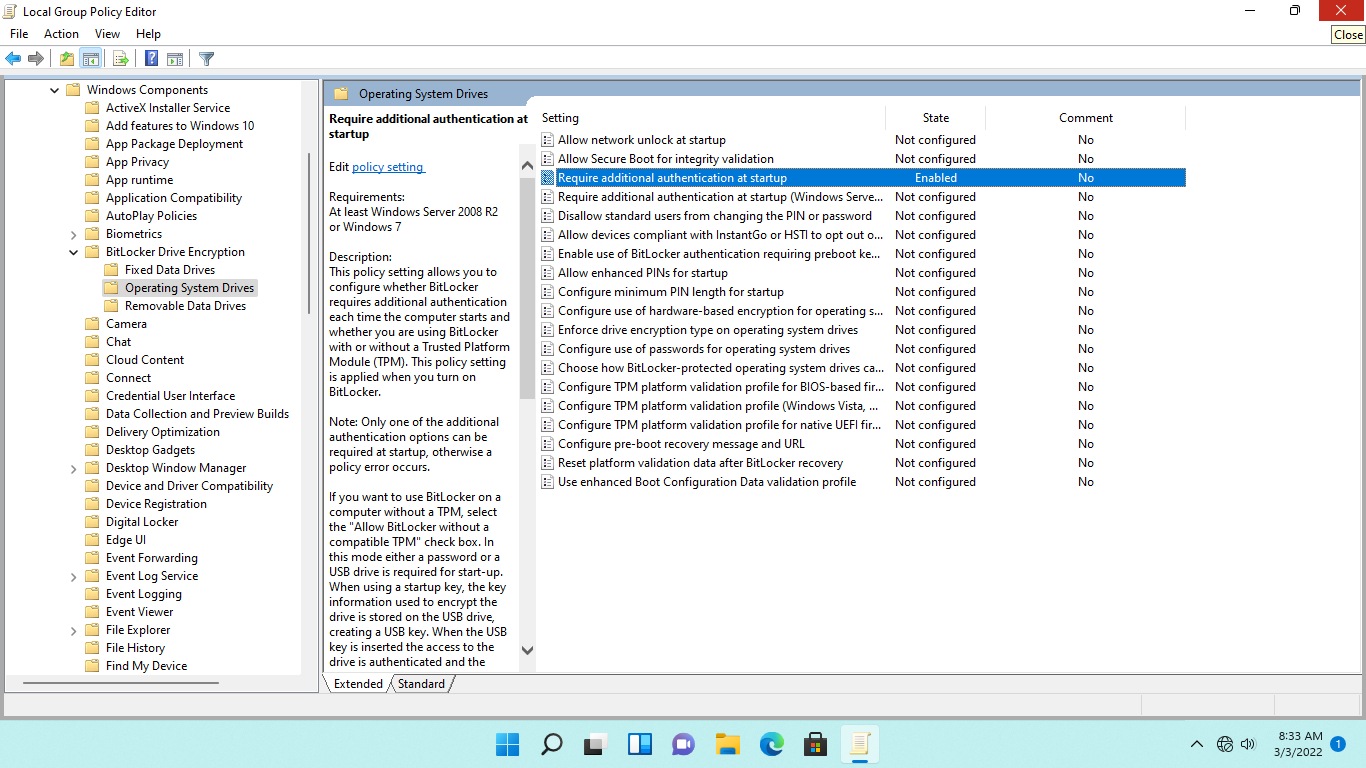
Keep the other default settings.

Click **OK** to save the changes.



**Step 4:**

Close the **Local Group Policy** **Editor** window.



## **Task 3: Encrypt Data Drive with BitLocker**

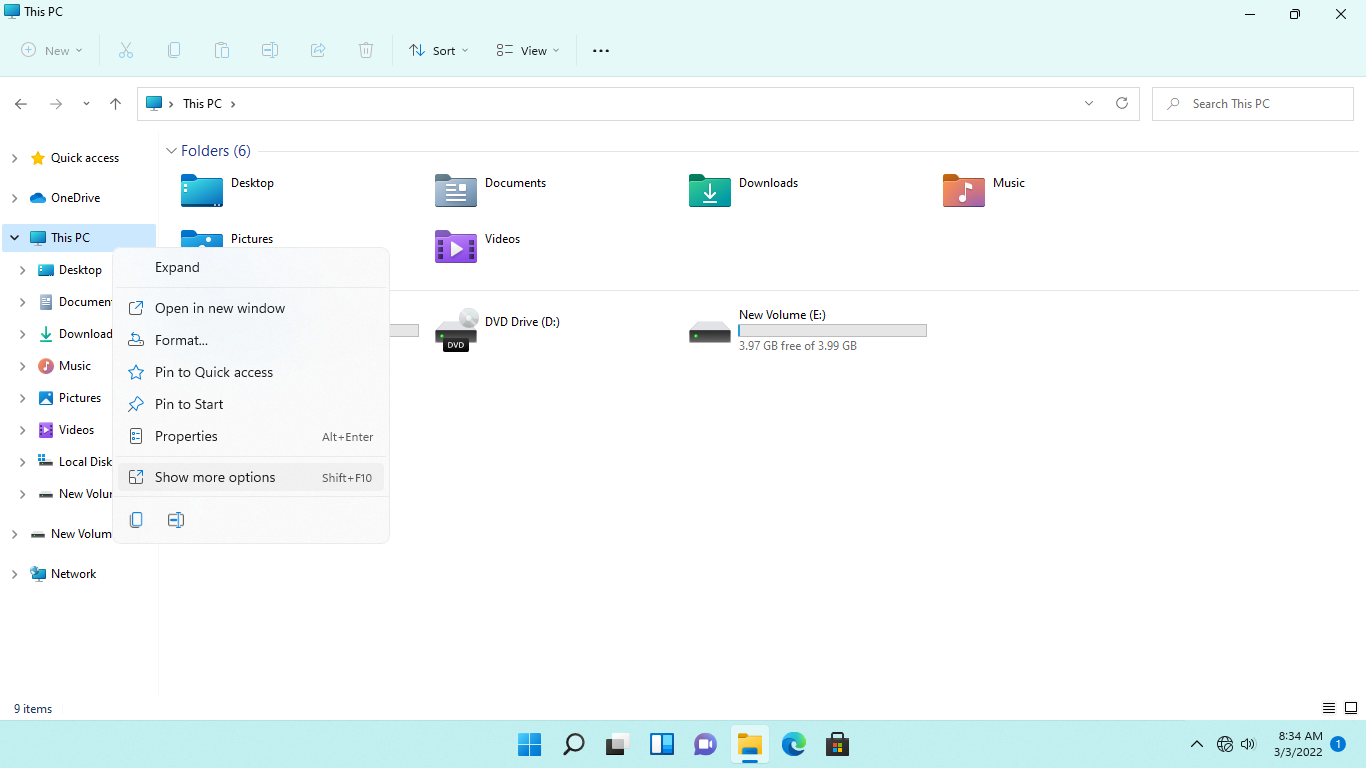
On NTWIN11VM1 without a TPM chip, you activated a group policy object configuration to support BitLocker.

In this task, we will encrypt the secondary hard disk - the E: drive on PLABWIN10 - using BitLocker.

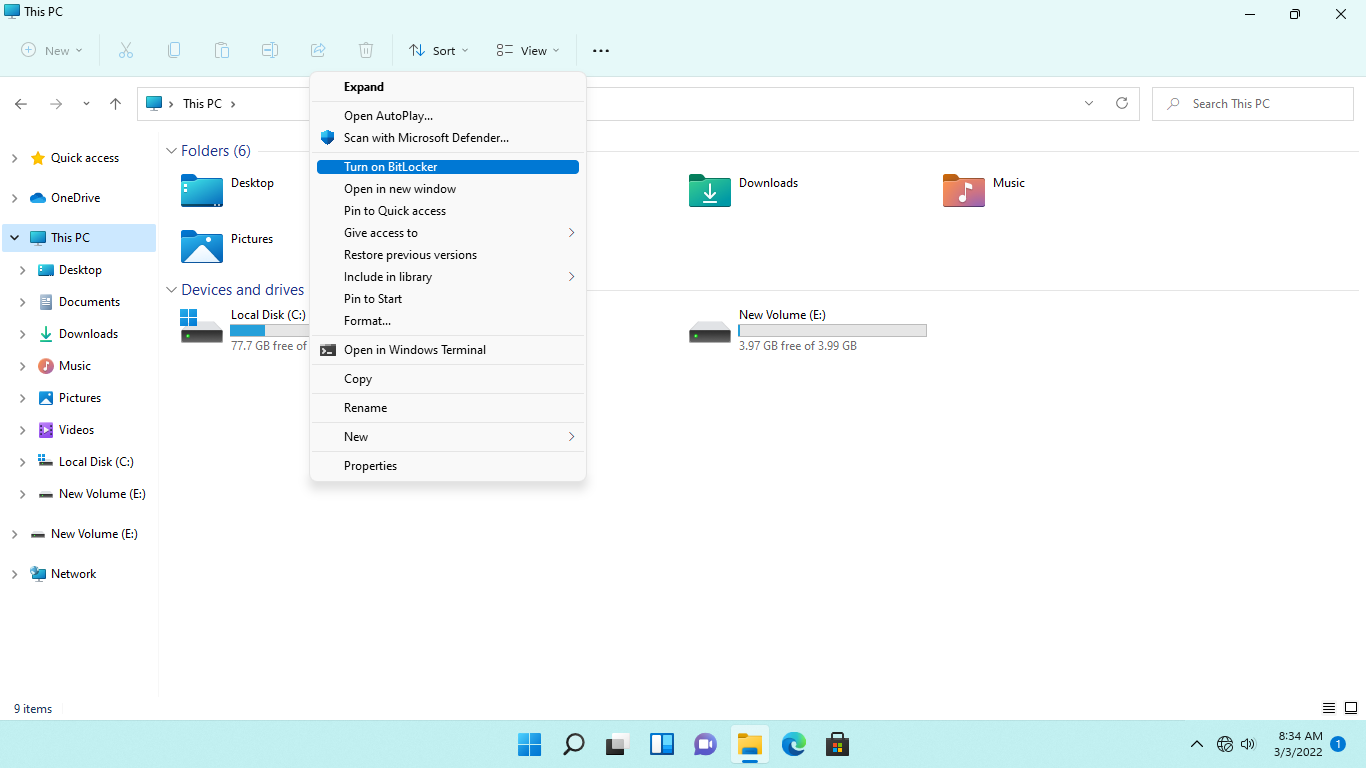
**Step 1:**

On **NTWIN11VM1** desktop, click **File Explorer** on the **Taskbar**.

Expand **This PC** and right-click **New Volume (E:)** then select **show more option.**



And select **Turn on BitLocker.**

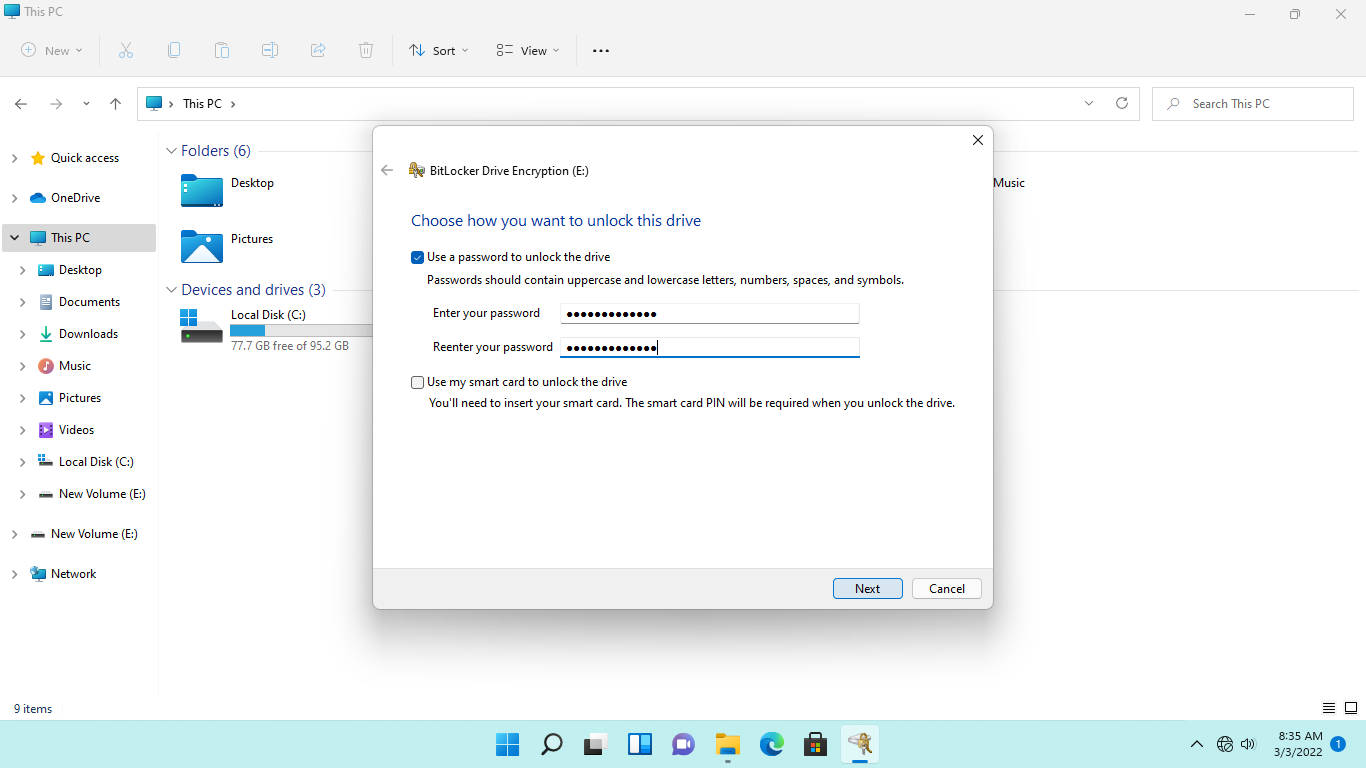


**Step 2:**

On the BitLocker Drive Encryption (E:) - Choose how you want to unlock this drive page, tick the Use a password to unlock the drive checkbox.

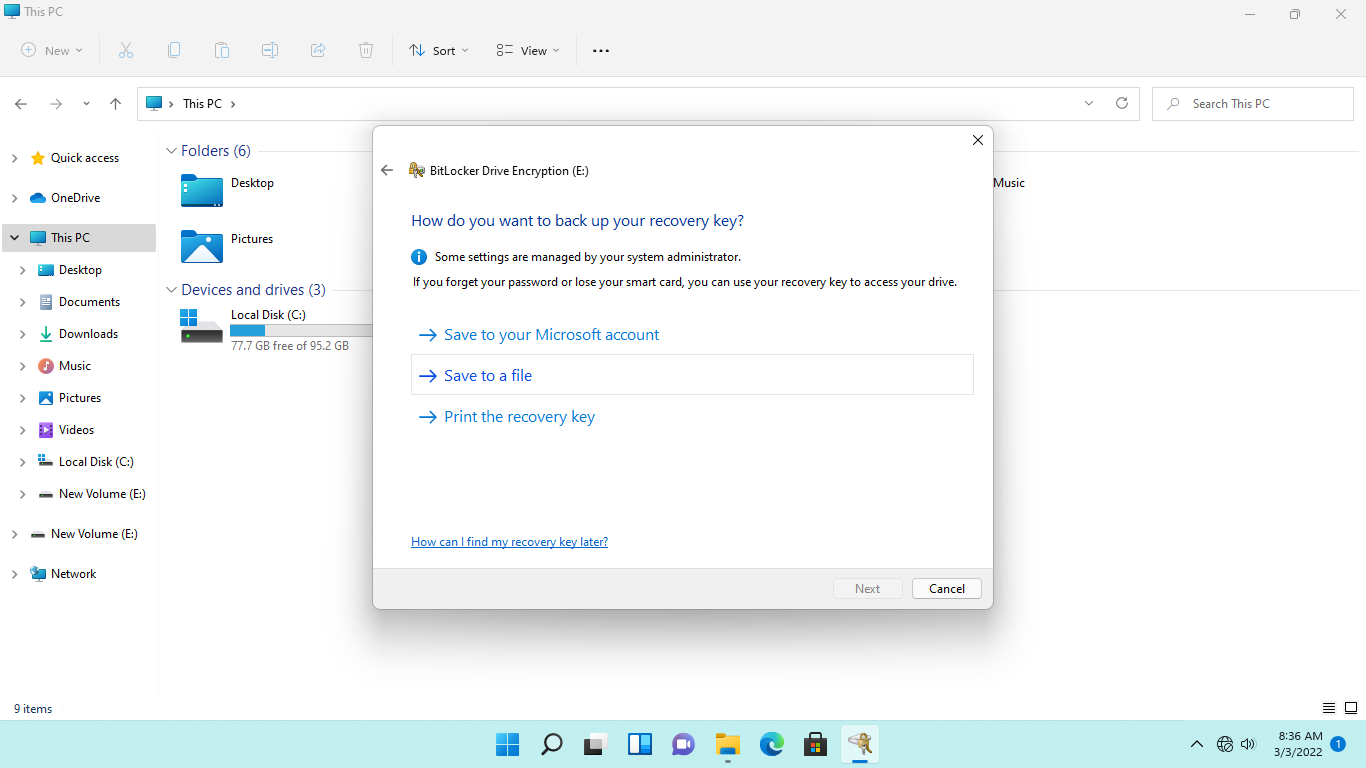
In the Enter your password and Reenter your password textboxes, type: ***Networktute@1***

Click **Next**.



**Step 3:**

On the **How do you want to back up your recovery key** page, select **Save to a file**.



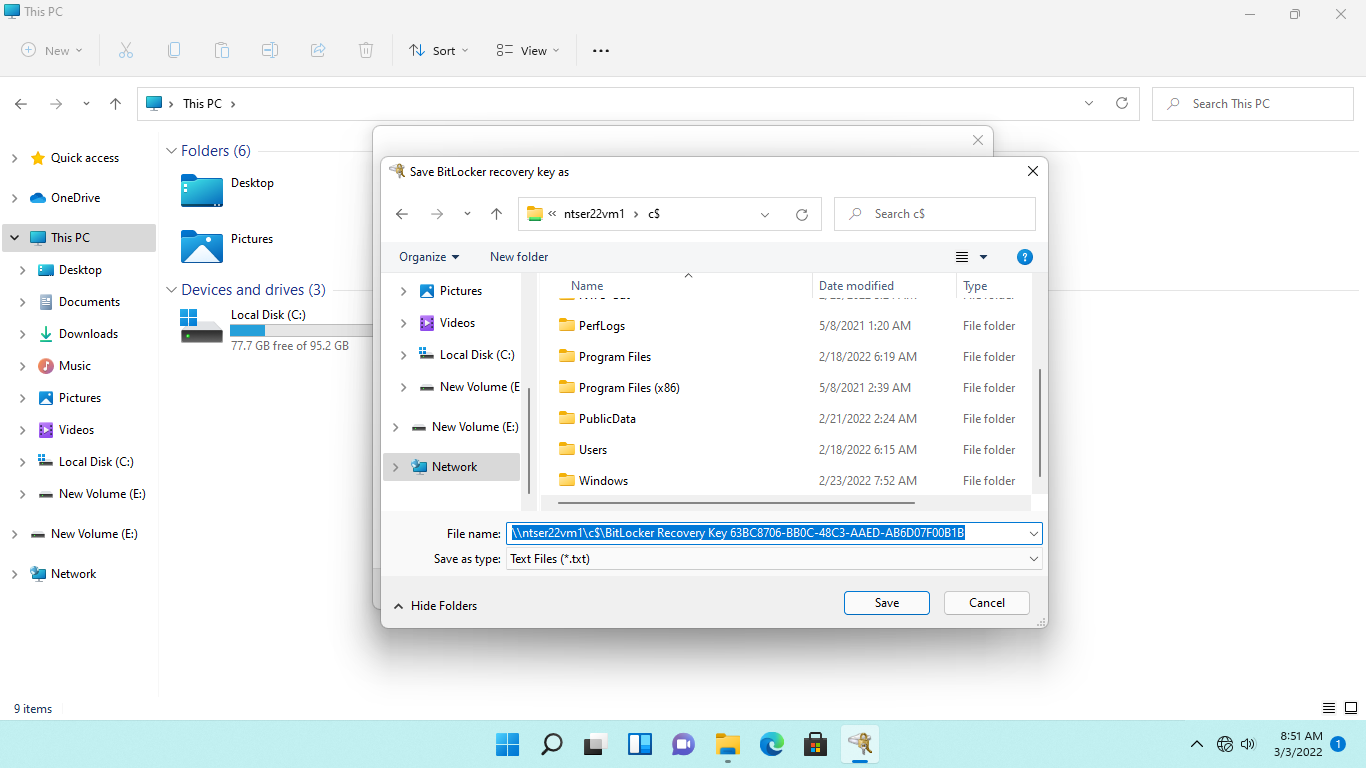
**Step 4:**

On the Save BitLocker recovery keys as dialog box, you must save the recovery key on another computer.

Click at the beginning of the provided file name and type: ***\\plabdc01\c$\***

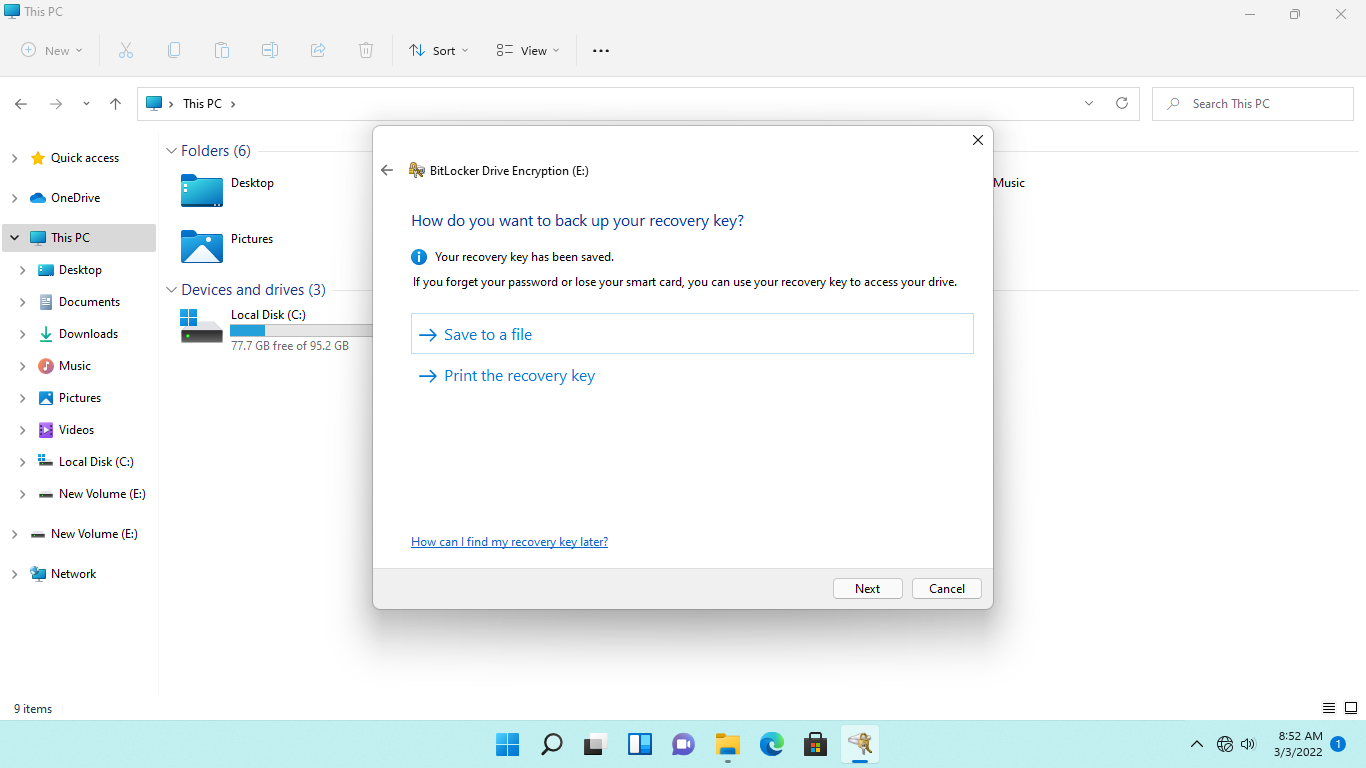
You will use the provided file name in the text box.

Click **Save.**



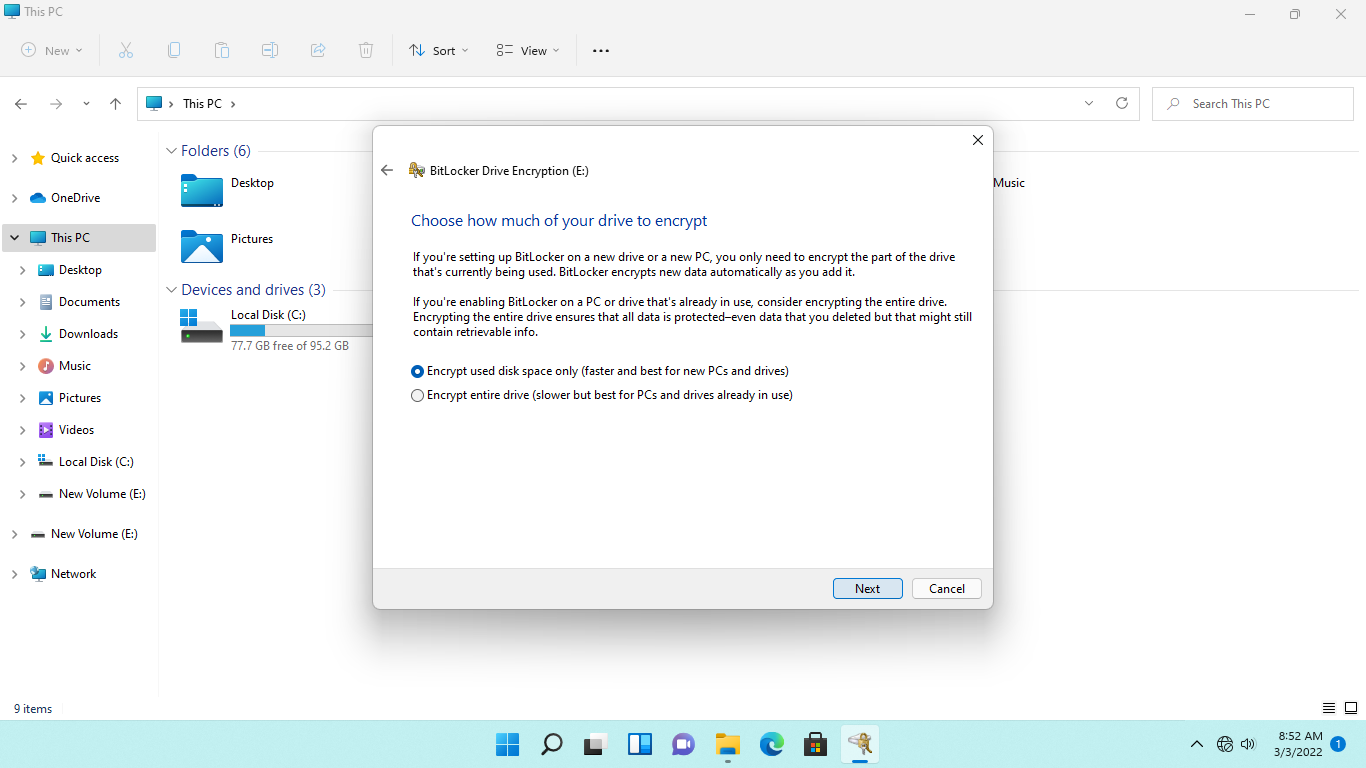
**Step 5:**

Back on the **How do you want to back up your recovery key** page, click **Next.**



**Step 6:**

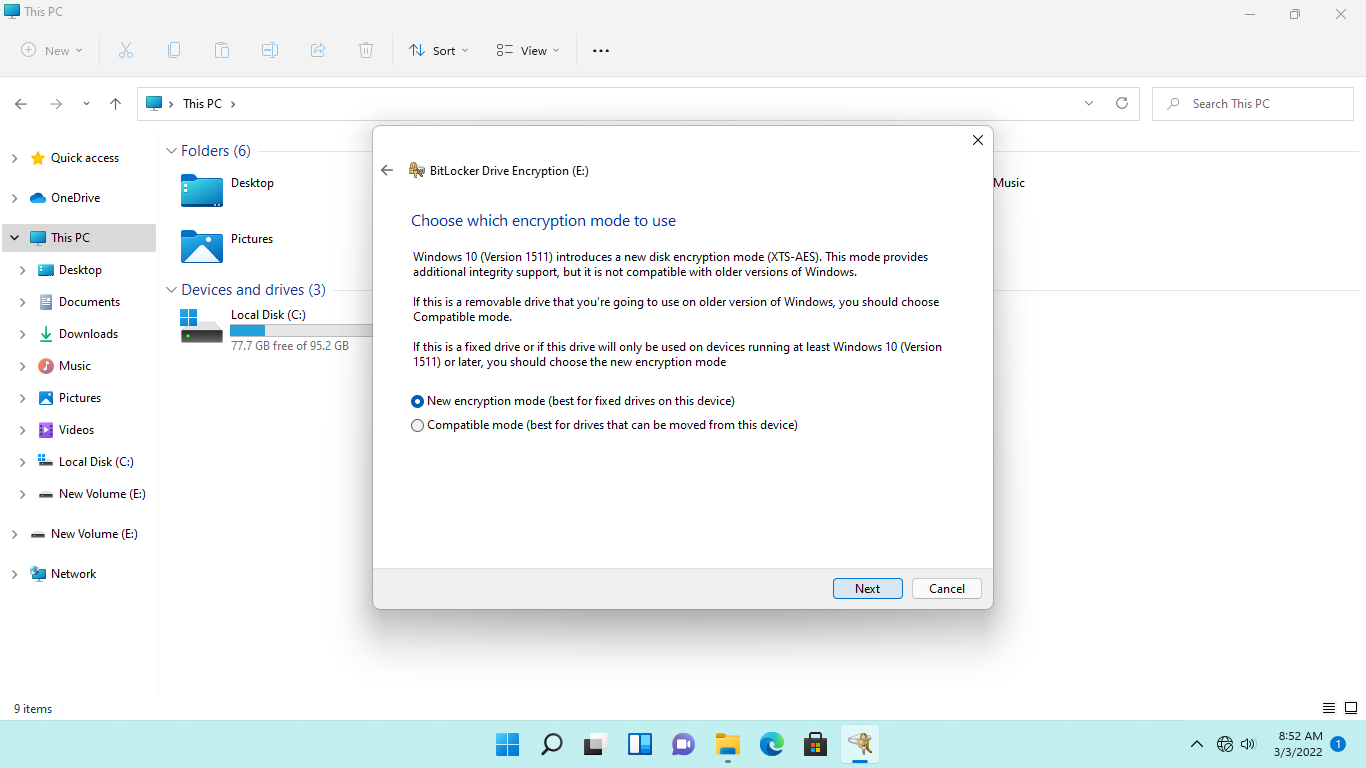
On the **Choose how much your drive to encrypt**, click **Next**.



**Step 7:**

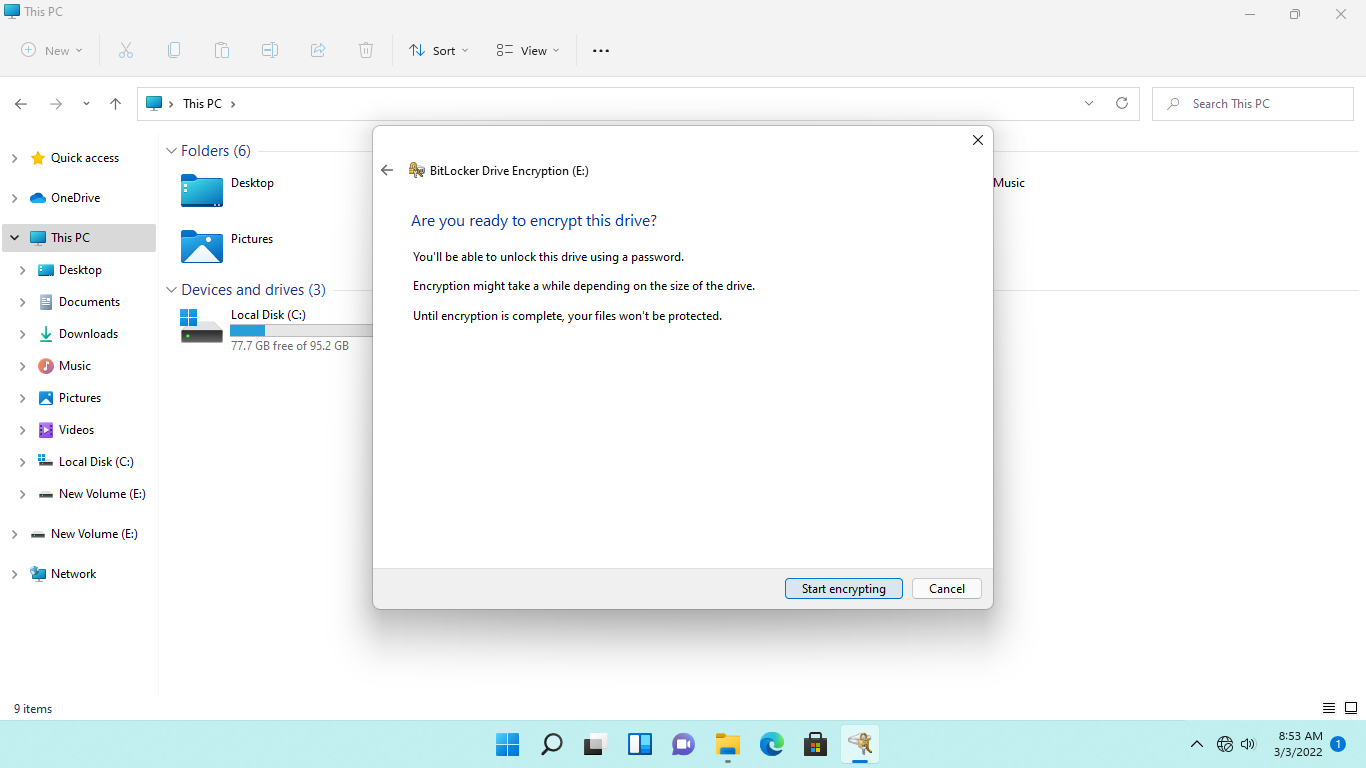
On the **Choose which encryption mode to use** page, keep the default selection.

Click **Next**.



**Step 8:**

On the **Are you ready to encrypt this drive** page, click **Start encrypting**.



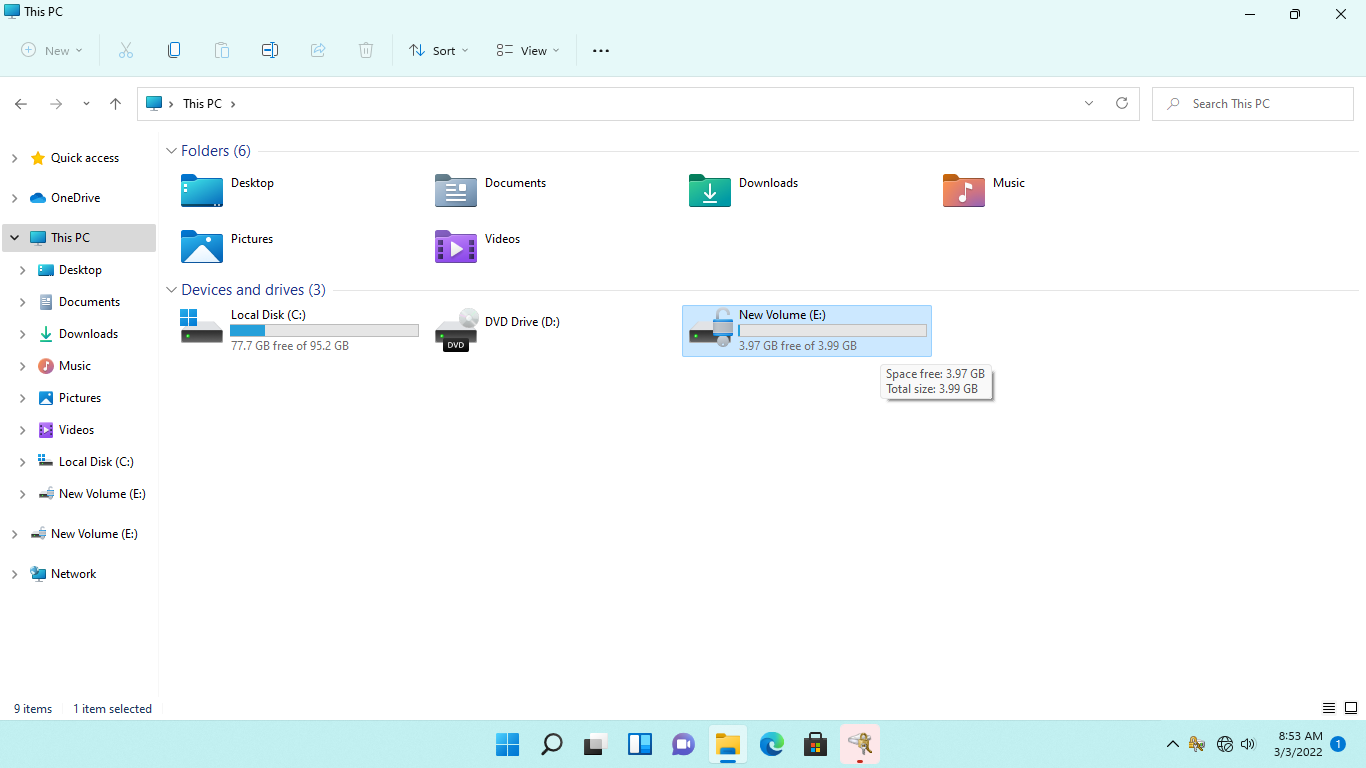
**Step 9:**

Please wait while **BitLocker** starts the encryption of the E: drive.

After a few seconds, click **This PC** node.

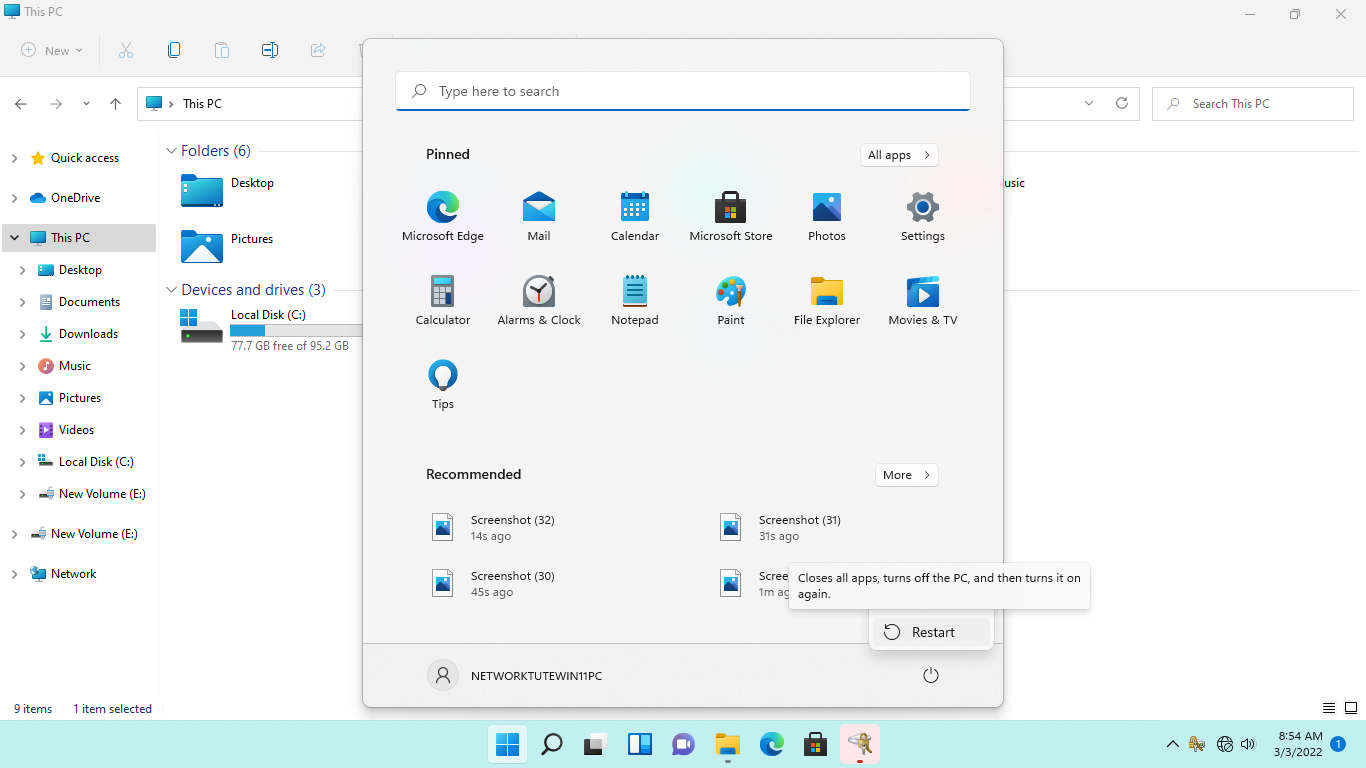
Notice that an unlocked padlock icon is appears on the **New Volume E** drive. However, you need to restart the computer to let **BitLocker** finish the encryption process on the new volume.

Close **File Explorer** window.



**Step 10:**

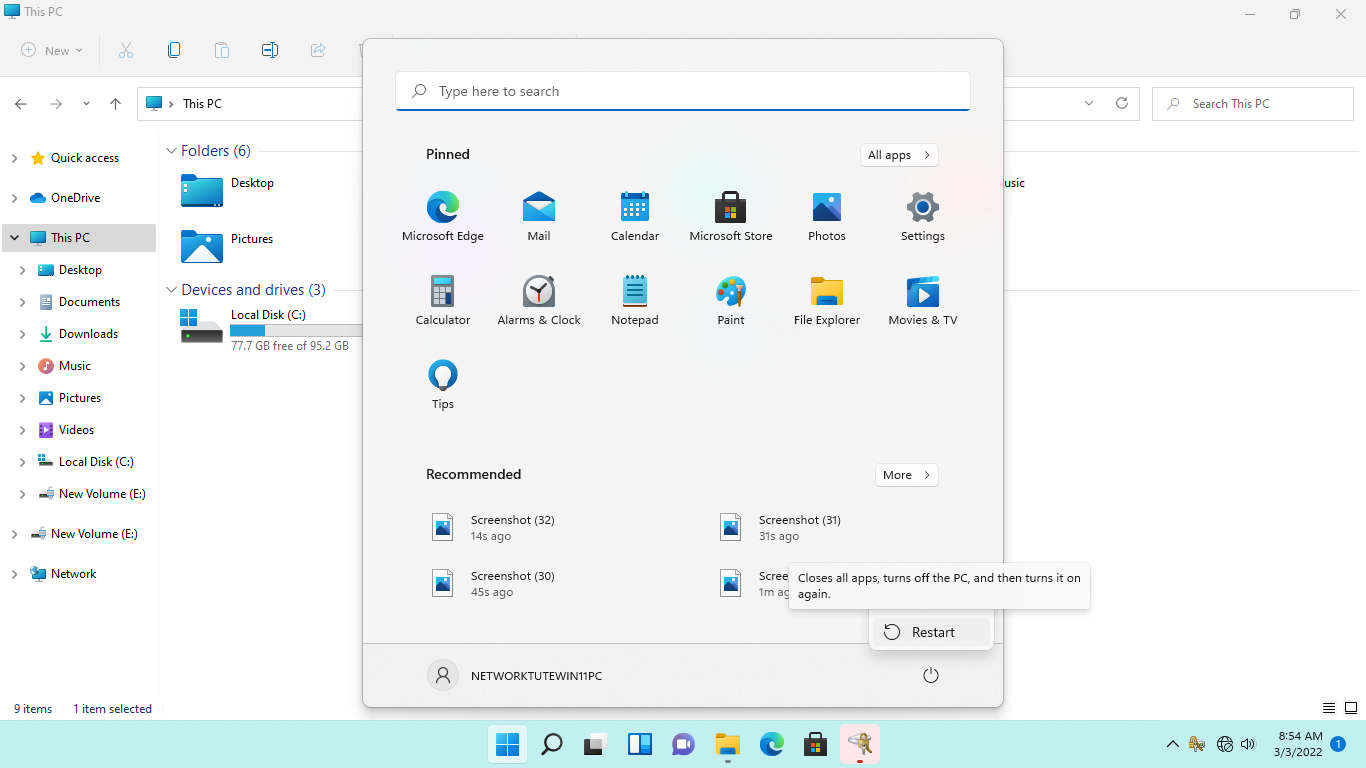
Click the **Start** icon, point to **Shut down or sign out** and select **Restart**.



**Step 11:**

After 1 minute, reconnect to **NTWIN11VM1**.

When signed-in, click **File Explorer** on the **Taskbar**.

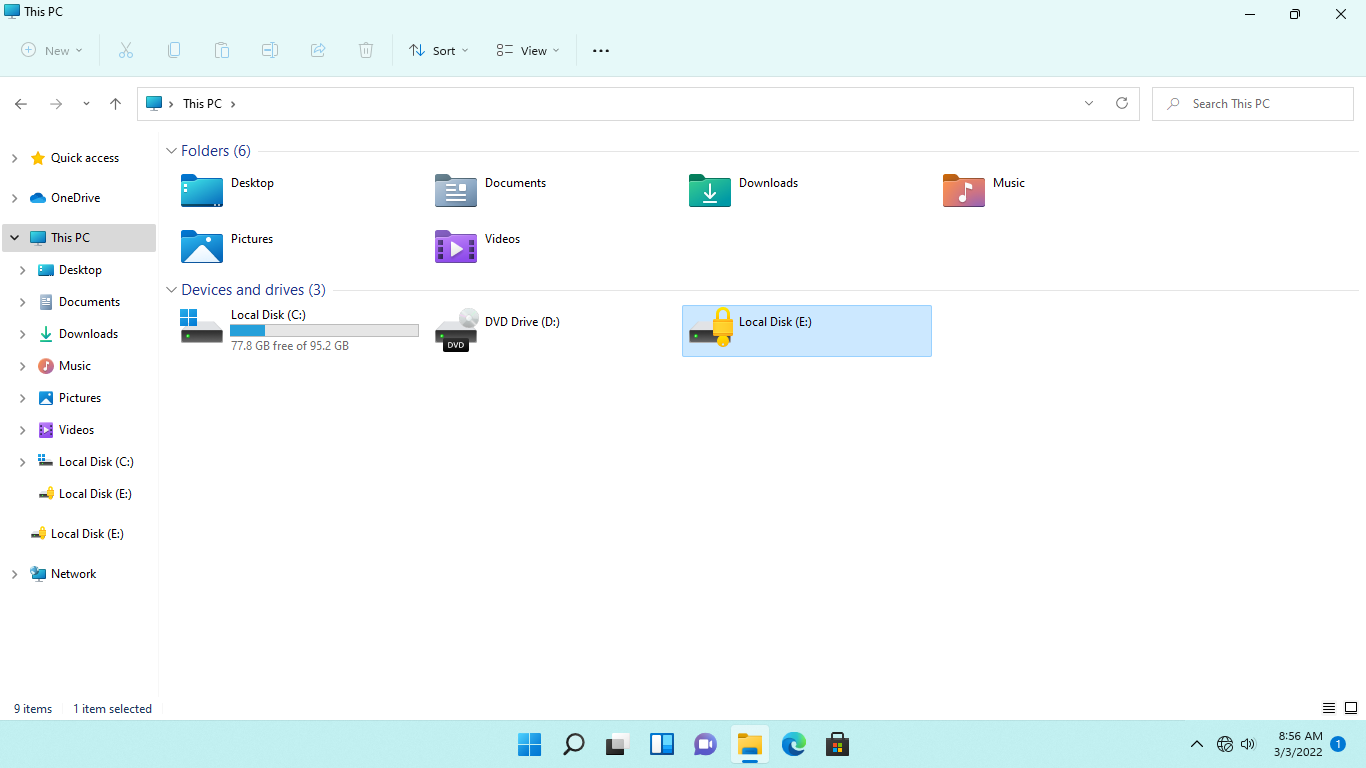


**Step 12:**

On the **File Explorer** window, click **This PC.**

Notice that a gold padlock icon is now appearing on the **E:** drive, meaning the **Local Disk (E:)** drive is now enabled for **BitLocker** encryption.

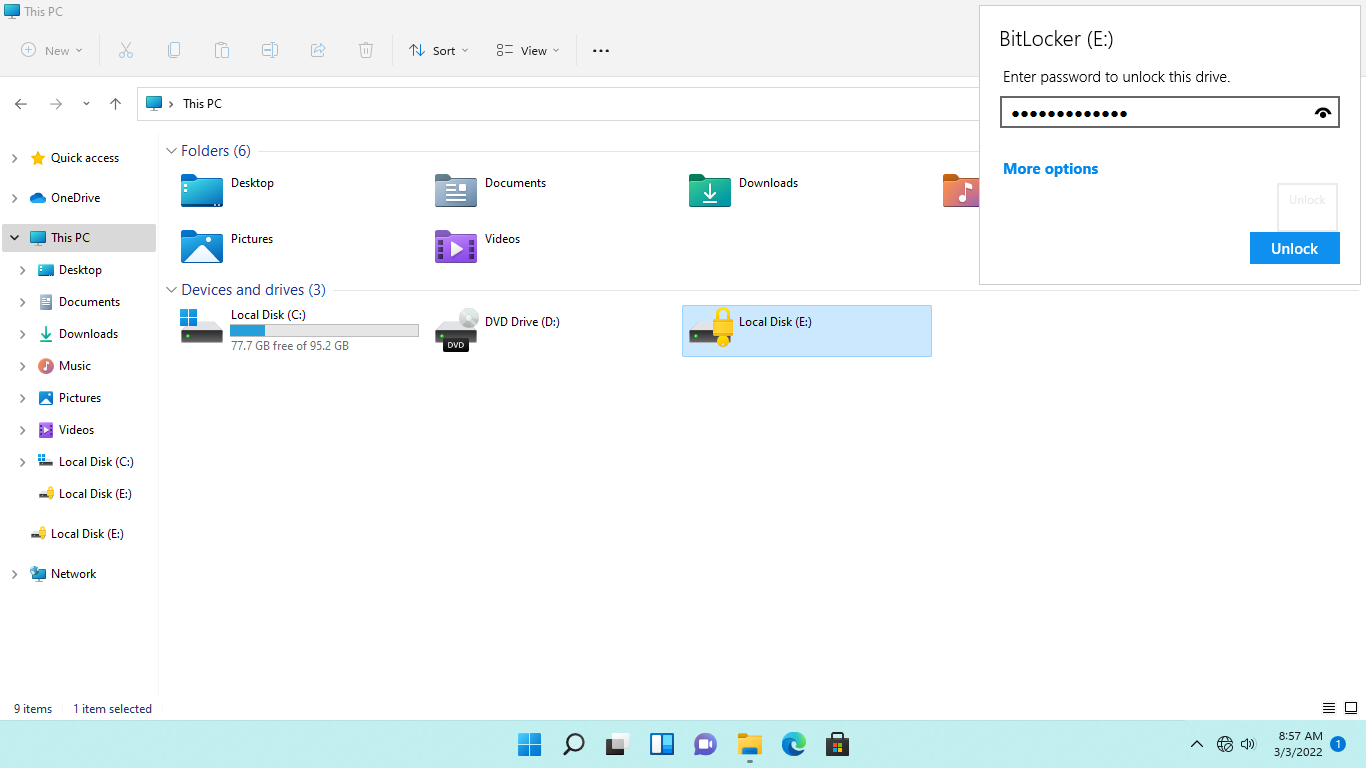
Double-click the **Local Disk (E:)** drive.



**Step 13:**

When the **BitLocker (D:)** dialog box appears, type: ***Networktute@1***

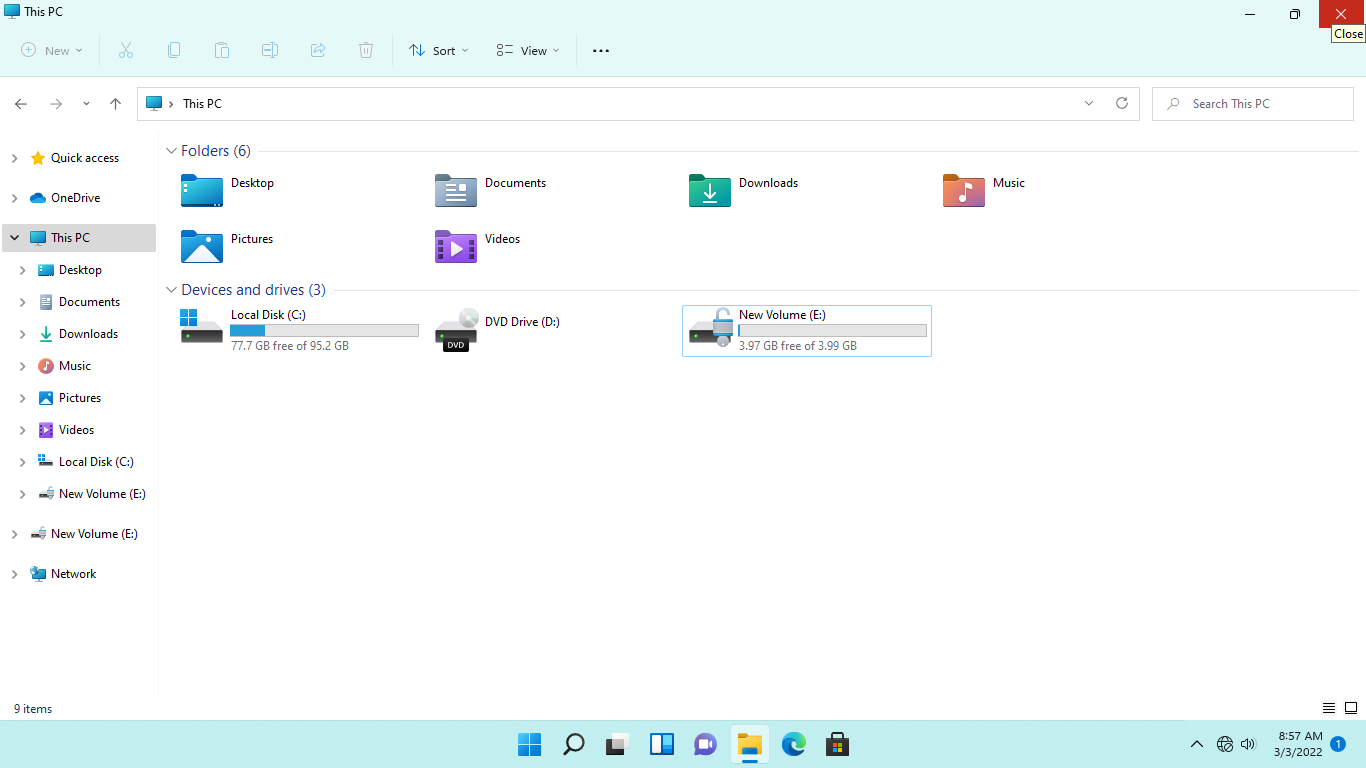
Click **Unlock**.



**Step 14:**

The **BitLocker** protected **E:** drive is now unlocked.

Close **File Explorer.**



## **Task 4: Manage BitLocker-Enabled Drive with Manage-bde**

Apart from Control Panel and File Explorer, the command prompt tool supports the management of BitLocker-enabled drives with manage-bde.exe.

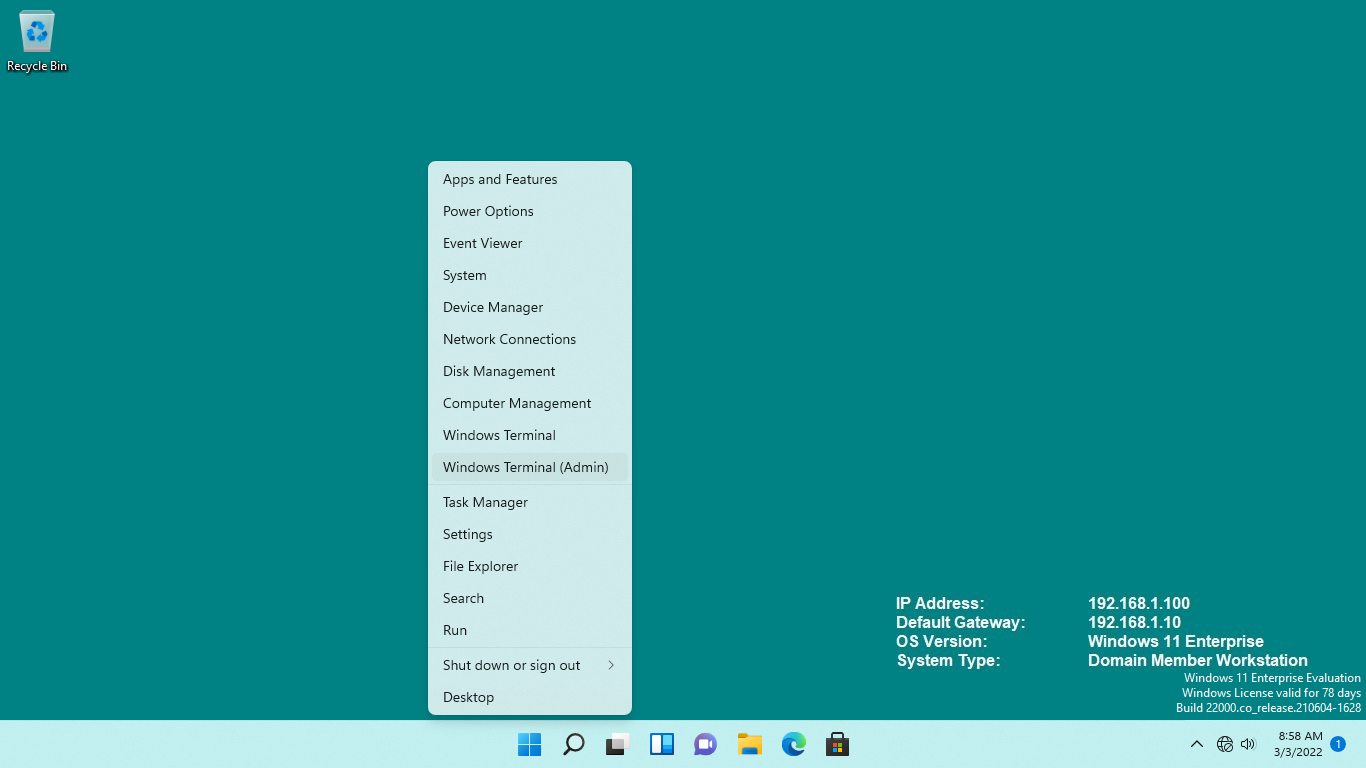
In this task, you will run the manage-bde tool to view the properties of a drive protected by BitLocker.

**Step 1:**

Ensure you are connected to **NTWIN11VM1**.

Right-click the **Start** icon, select **Windows PowerShell (Admin).**

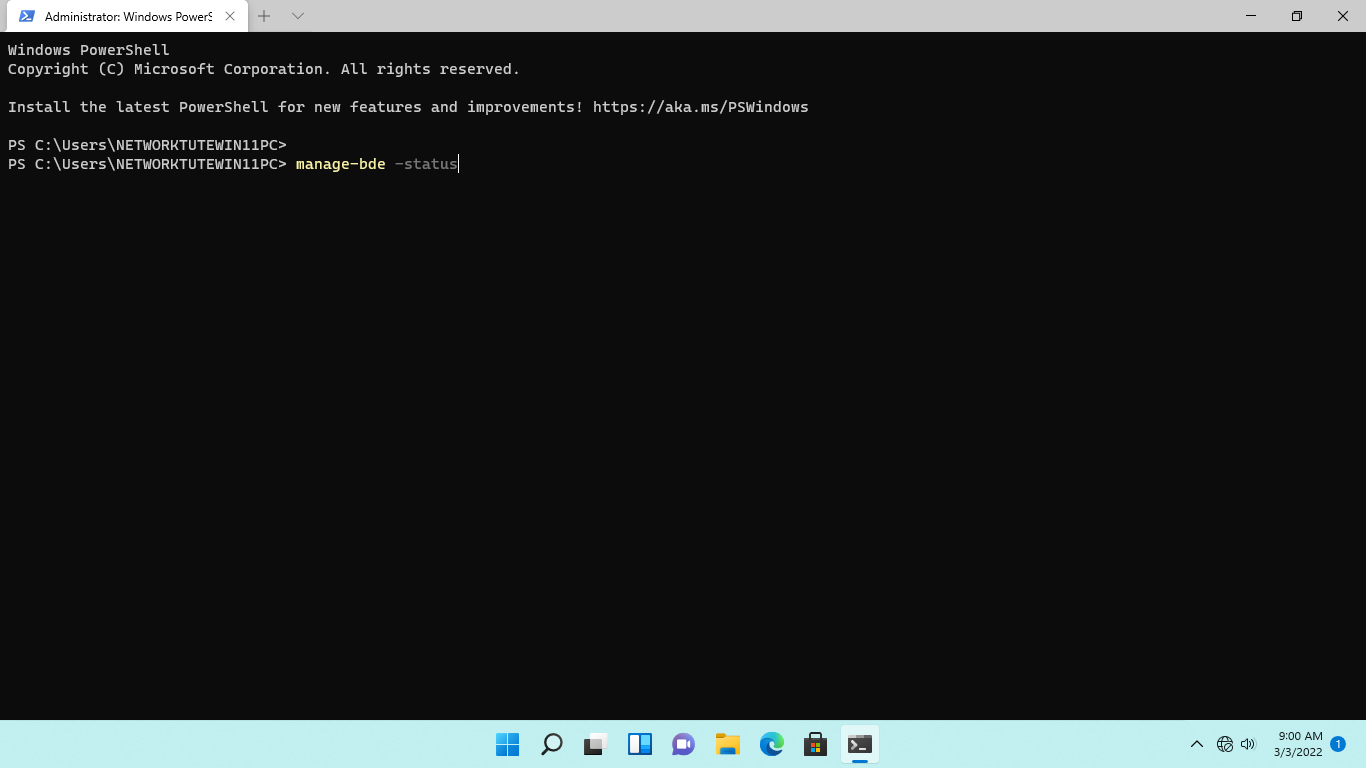
Click **Yes** if the **User Account Control** message box appears.



**Step 2:**

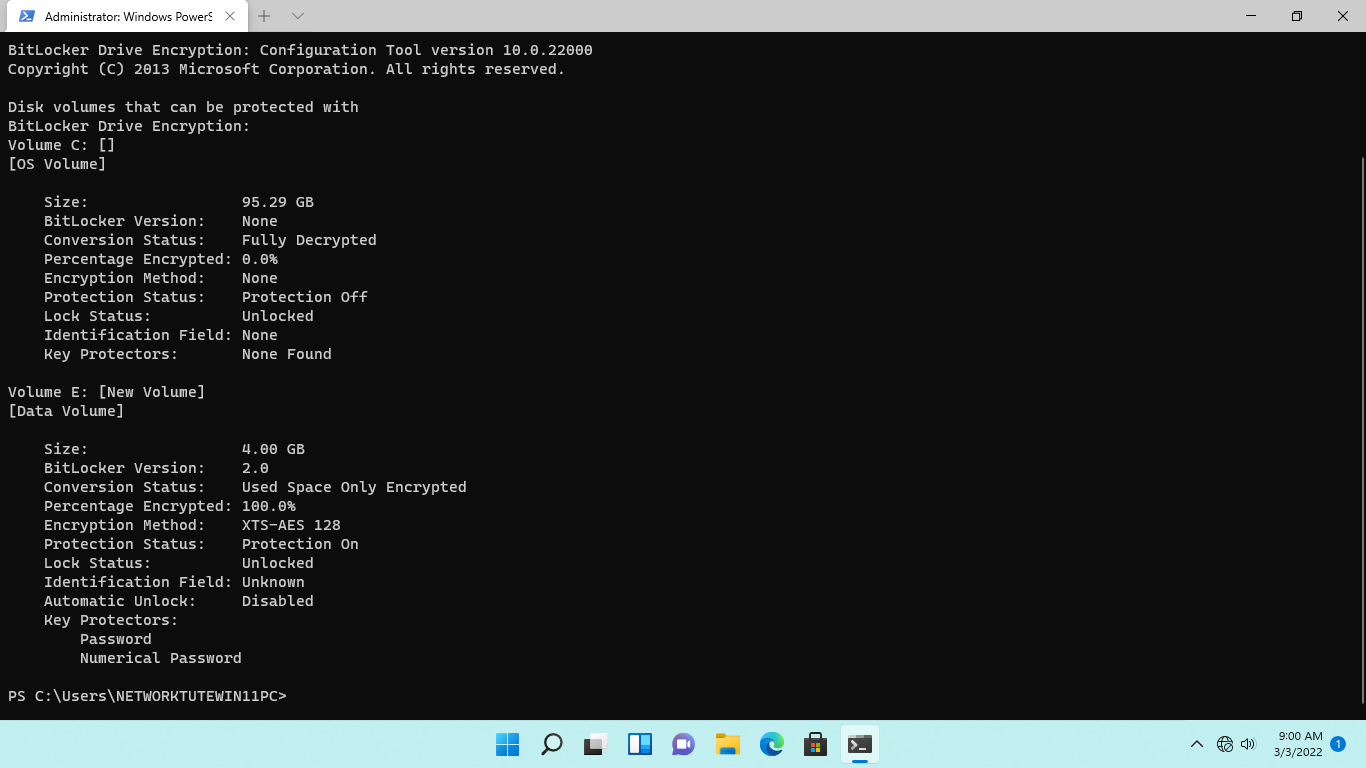
On **Windows PowerShell (Admin)**, type the following to get the status of the fixed drives: ***manage-bde -status***

Press **Enter**.



**Step 3:**

**Windows PowerShell** displays the status of the fixed drives on **NTWIN11VM1.**

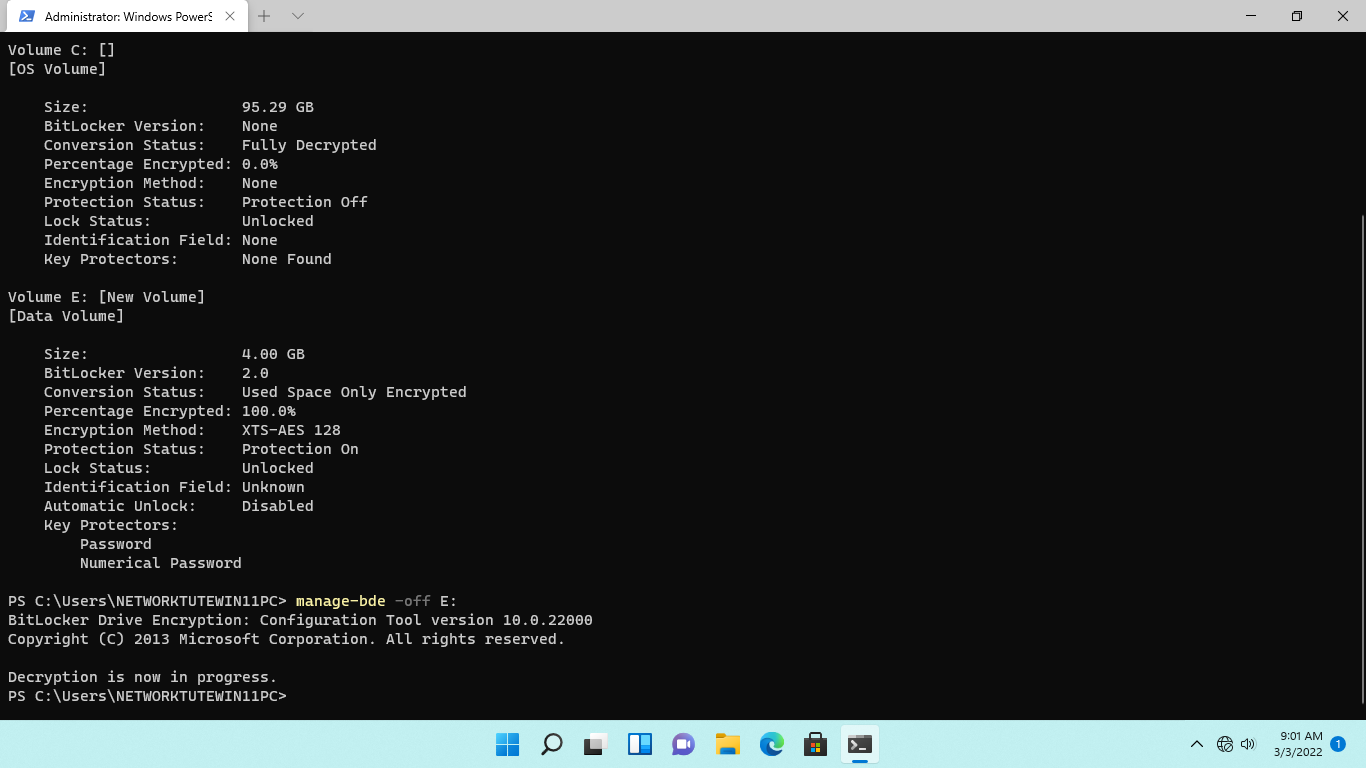


**Step 4:**

Scroll to the end of the status information.

On the next prompt, type the following command to decrypt drive E: ***manage-bde -off E:***

Press **Enter**.



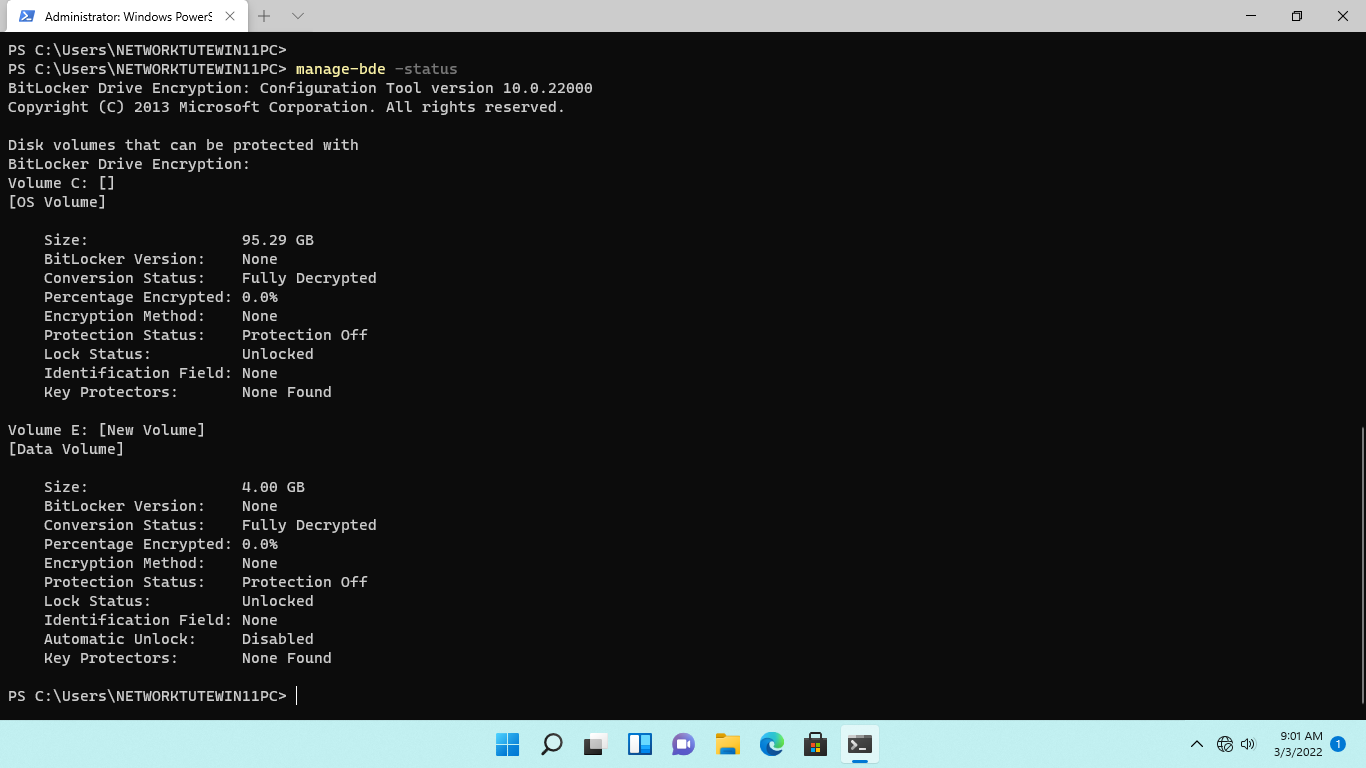
**Step 5:**

**Windows** will begin the decryption of the E: drive.

Please note that decryption will immediately take effect on the drive as it is empty at the moment.

On the next prompt, to verify the status of the fixed drives, type: ***manage-bde -status***

Press **Enter**.



**Step 6:**

Close **Windows PowerShell**.

|  |
| --- |
| Leave all devices powered on and continue to the next exercise. |