# **Exercise 1 - Automating Tasks with Task Scheduler.**

BitLocker is a security tool that encrypts the entire hard drive and protects the operating system. As in the case of servers running Active Directory Domain Services, operating system disks hold crucial information about the company.

Users' email messages are stored in a database on application servers that run messaging platforms, which might be a concern if the server's disk volume is hijacked or stolen.

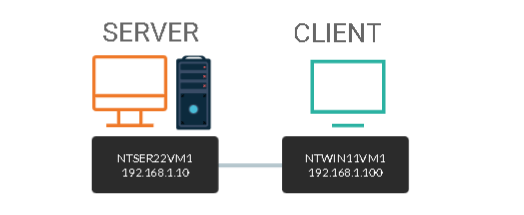
With business servers safeguarded in data centers, it's critical to add security layers by encrypting Windows' system disk.

Let’s now encrypt the system drive of a Windows 10 computer.

In this exercise,

1. Enable Local Group Policy for BitLocker
2. Encrypt System Drive with BitLocker

## **Topology**



DOMAIN = networktute.com

NTSER22VM1 = Windows Server 2022 – Domain Controller

NTWIN11VM1 = Windows 11 – Domain Member

NTWIN10HV1 = Windows 11 Hyper-V VM

## **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: Start Guest Virtual Machine**

It was not possible to display the procedure of inputting the BitLocker password during the Windows 10 start-up on NTWIN10HV1 in the previous exercise. To demonstrate how BitLocker secures the system disk where the operating system data live, you'll utilize a guest virtual machine called NTWIN10HV1.

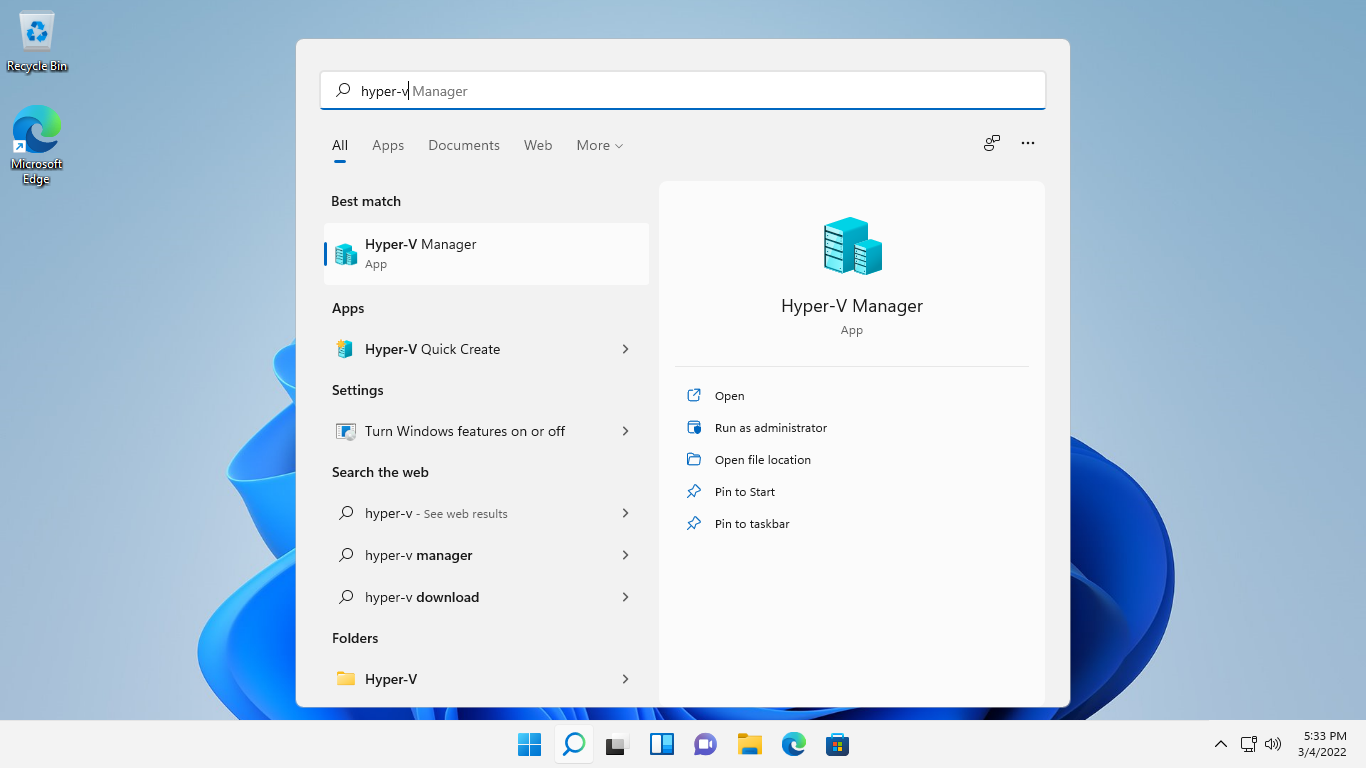
In this task, we will prepare the prerequisites to enable BitLocker on the system drive of NTWIN10HV1.

**Step 1:**

Connect to **NTWIN10HV1**.

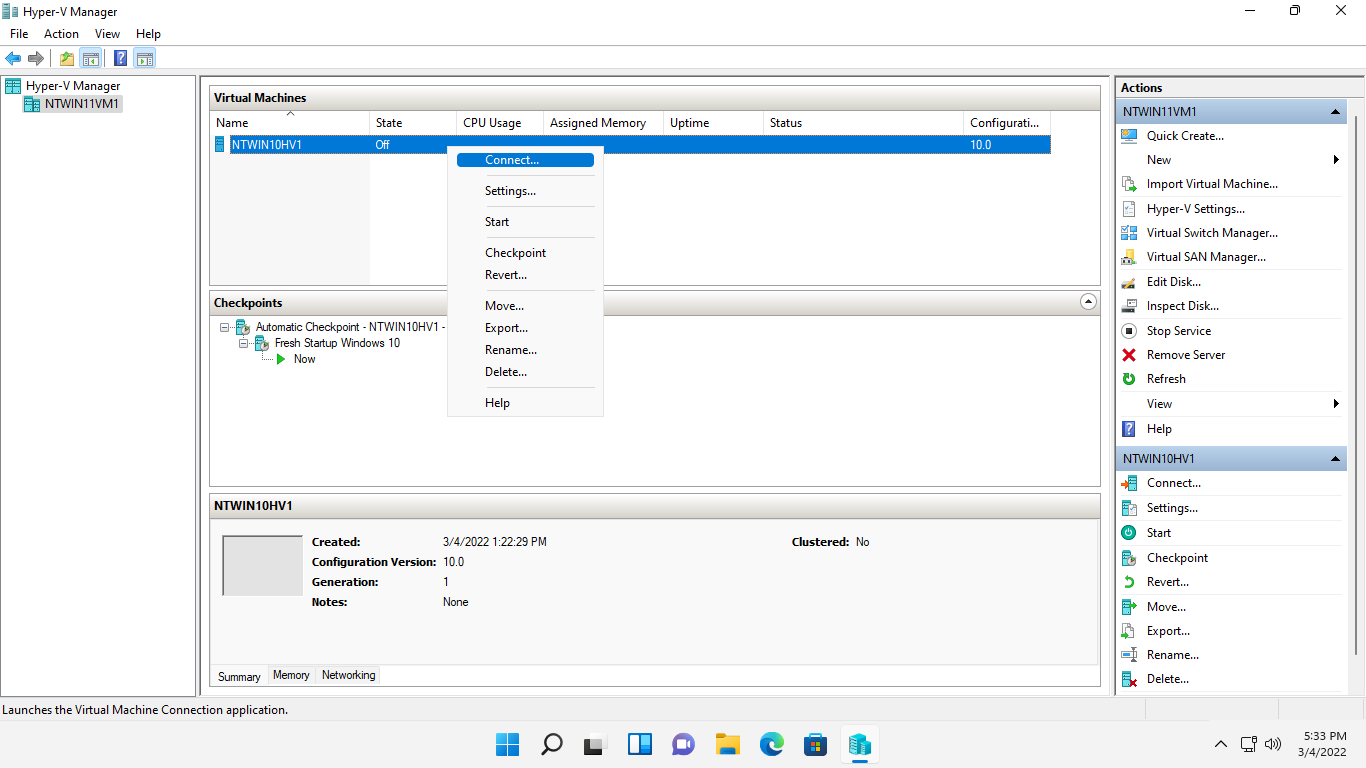
In the **Type here to search** textbox, type: ***hyper-v***

Under **Best Match**, select **Hyper-V Manager.**



**Step 2:**

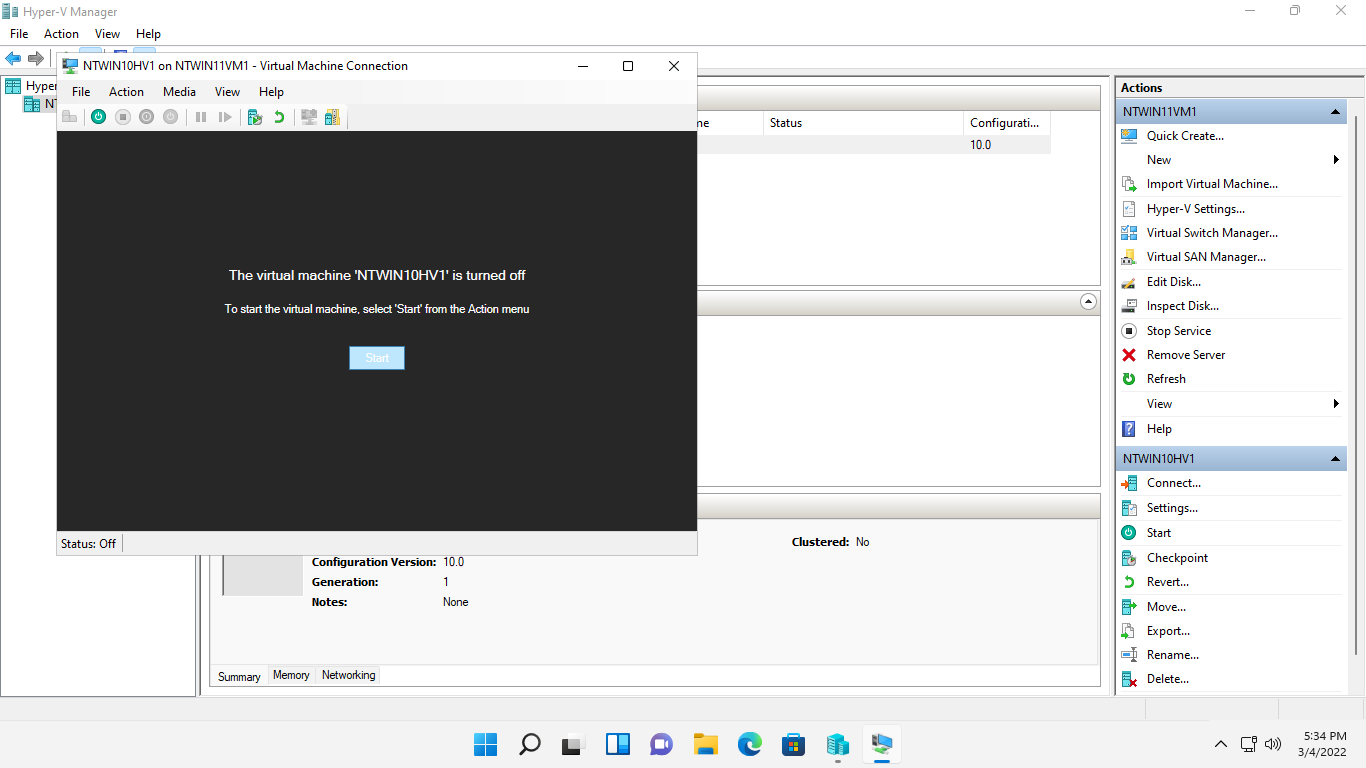
On the **Hyper-V Manager** window, under the **Virtual Machines** section, right-click **NTWIN10HV1** and select **Connect**.



**Step 3:**

The **NTWIN10HV1**on **NTWIN11VM1** - Virtual Machine Connection window opens.

Click **Start**.



**Step 4:**

Please wait while the **NTWIN10HV1** on guest virtual machine is starts up.

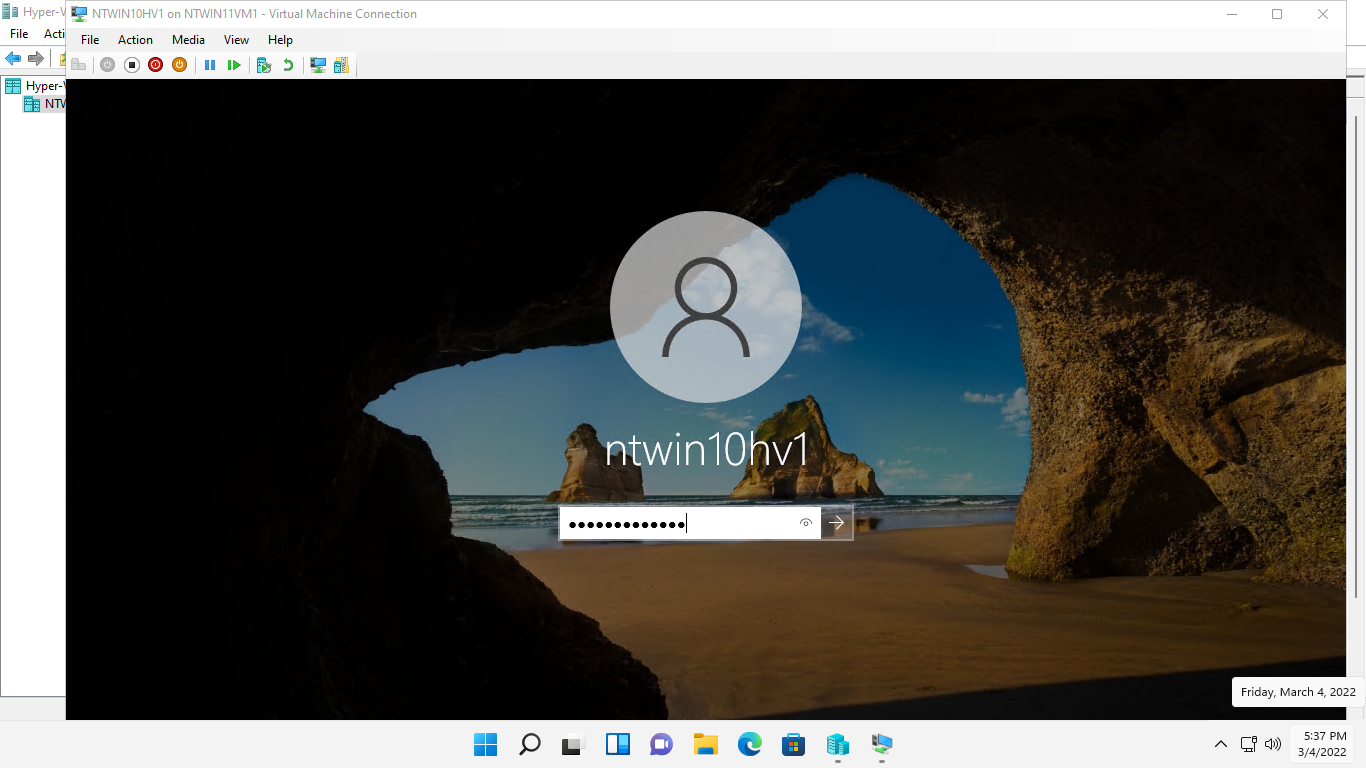
Click **Connect**.

Click **View** menu and select **Full Screen Mode**.

On the sign-in screen, **ntwin10hv1** is the default user.

In the Password box, type: ***Networktute@123***

Press **Enter.**



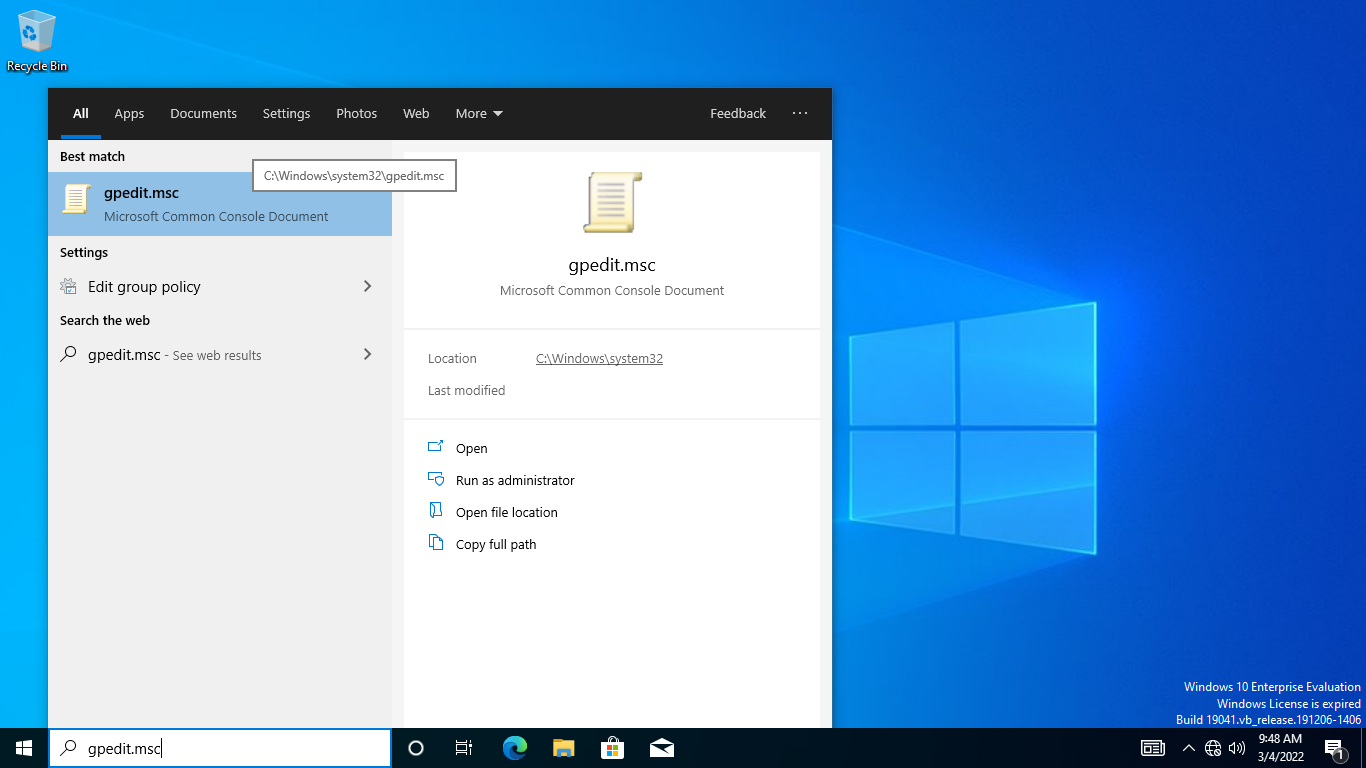
## **Task 2: Enable Local Group Policy for BitLocker**

In this task, we will enable a group policy setting to bypass the detection of a TPM chip that occurs when a drive is encrypted with BitLocker.

**Step 1:**

On the **NTWIN10HV1** desktop, click in the Ask me anything box and type: ***gpedit.msc***

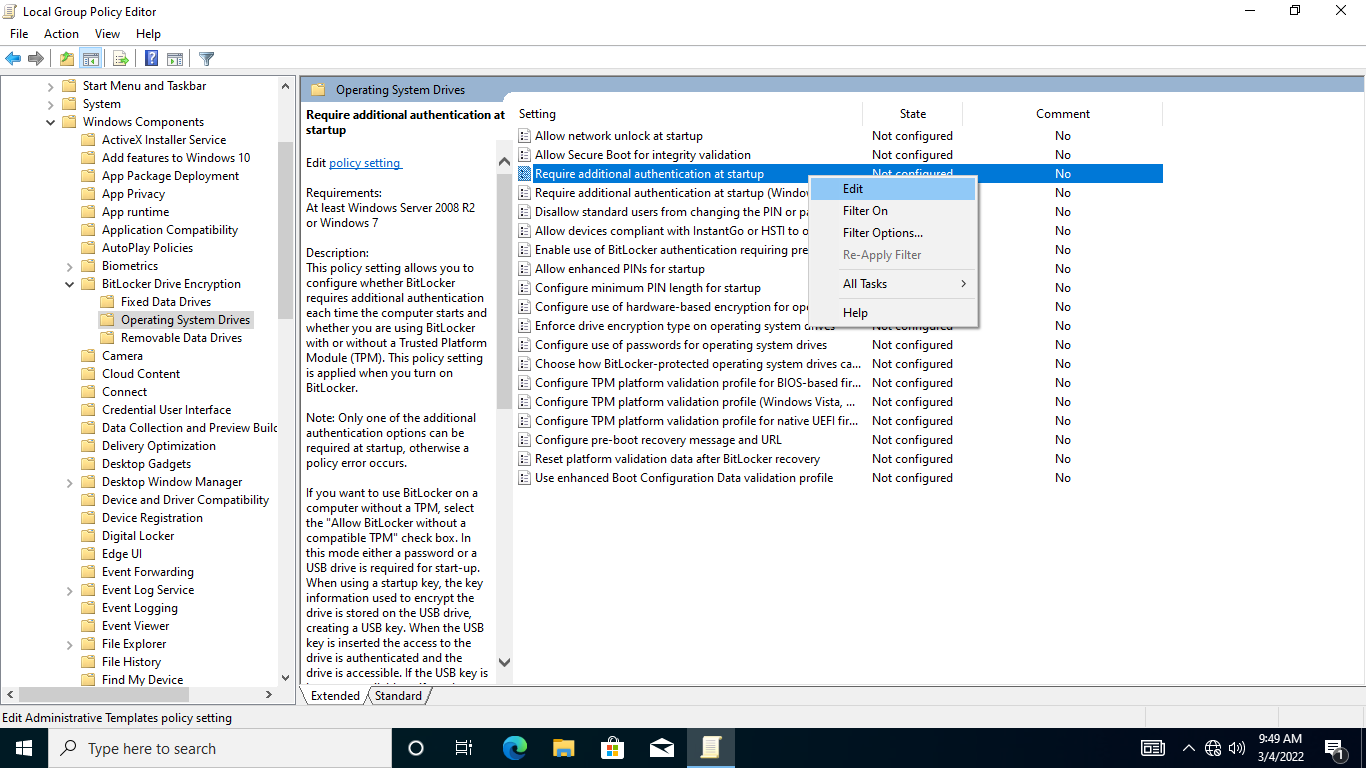
Press **Enter**.



**Step 2:**

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

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



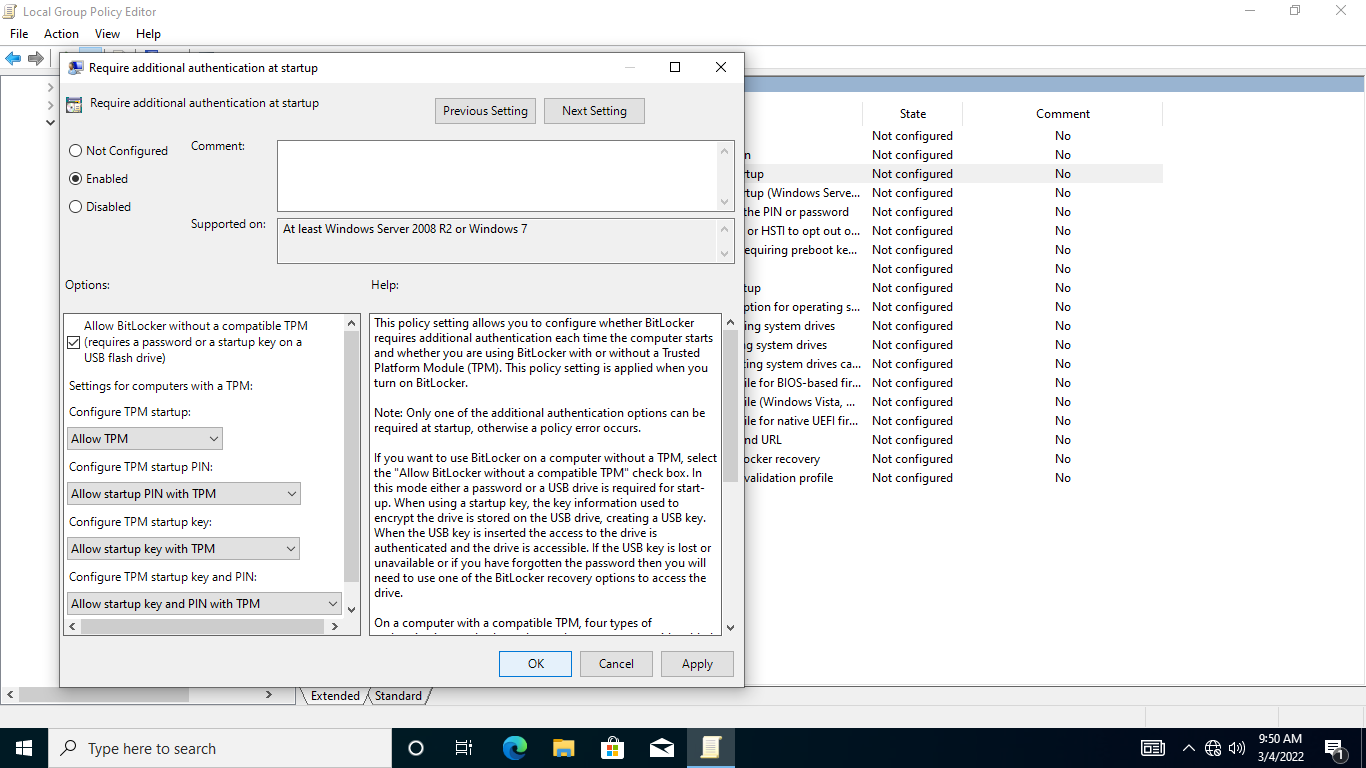
**Step 3:**

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

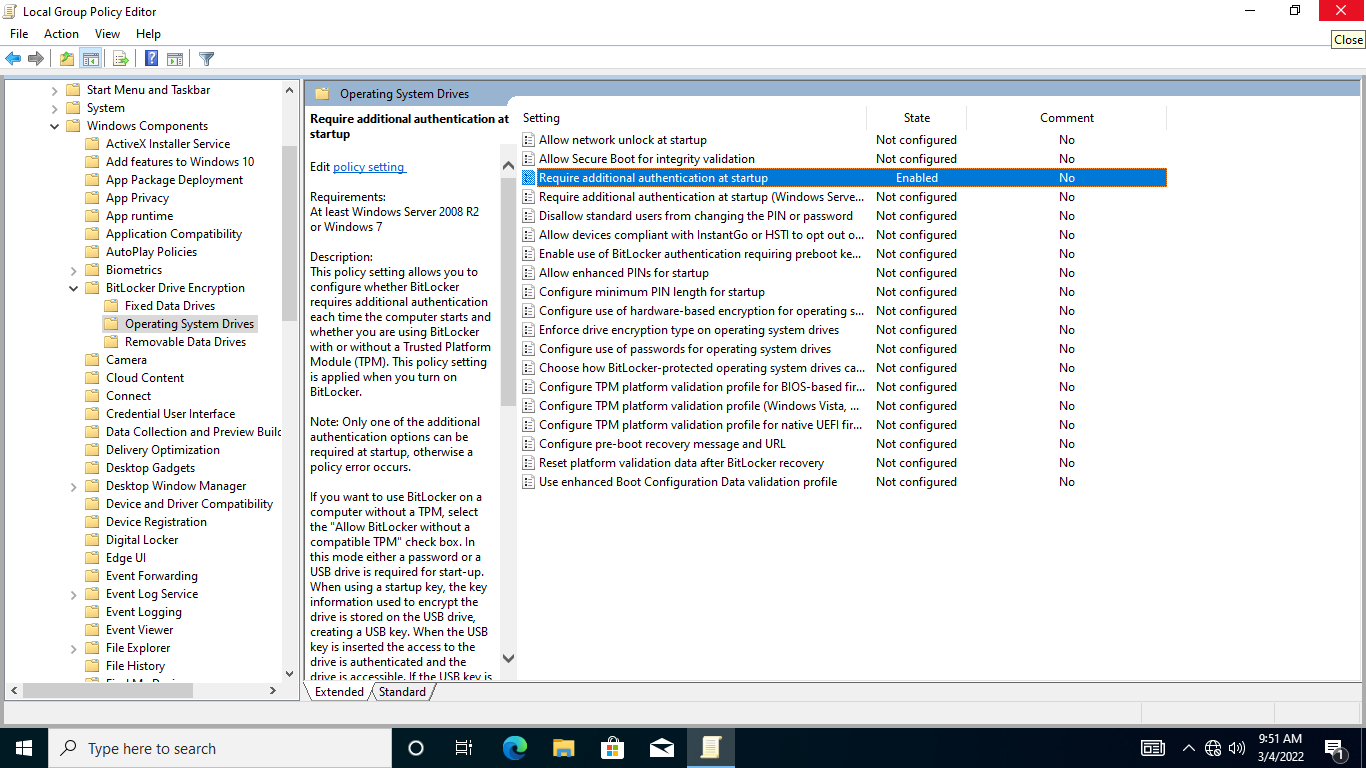
Keep the other default settings.

Click **OK** to save the changes and exit the dialog box.



**Step 4:**

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



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

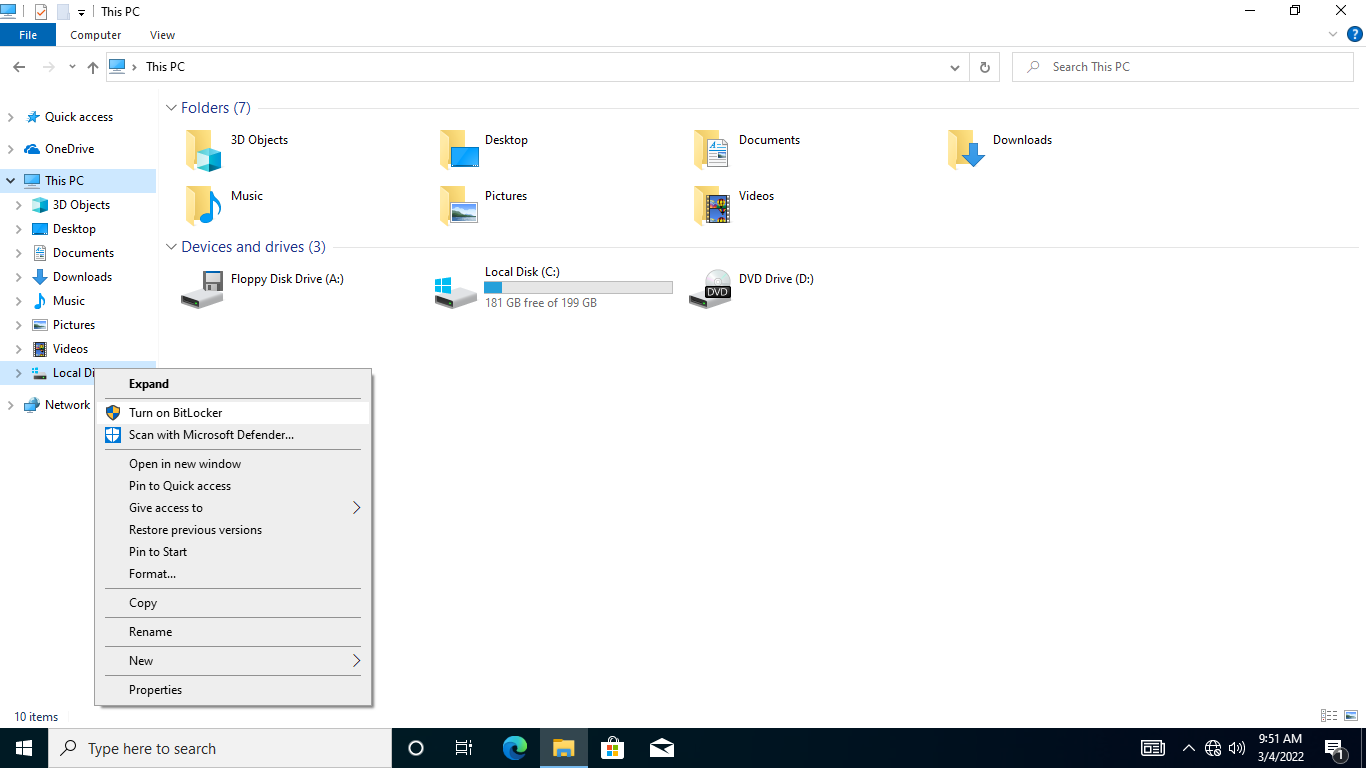
Once the system is ready to support BitLocker, you are ready to encrypt the operating system drive using BitLocker.

In this task, we will encrypt the Local Disk (C:) drive that contains the operating system data with BitLocker.

**Step 1:**

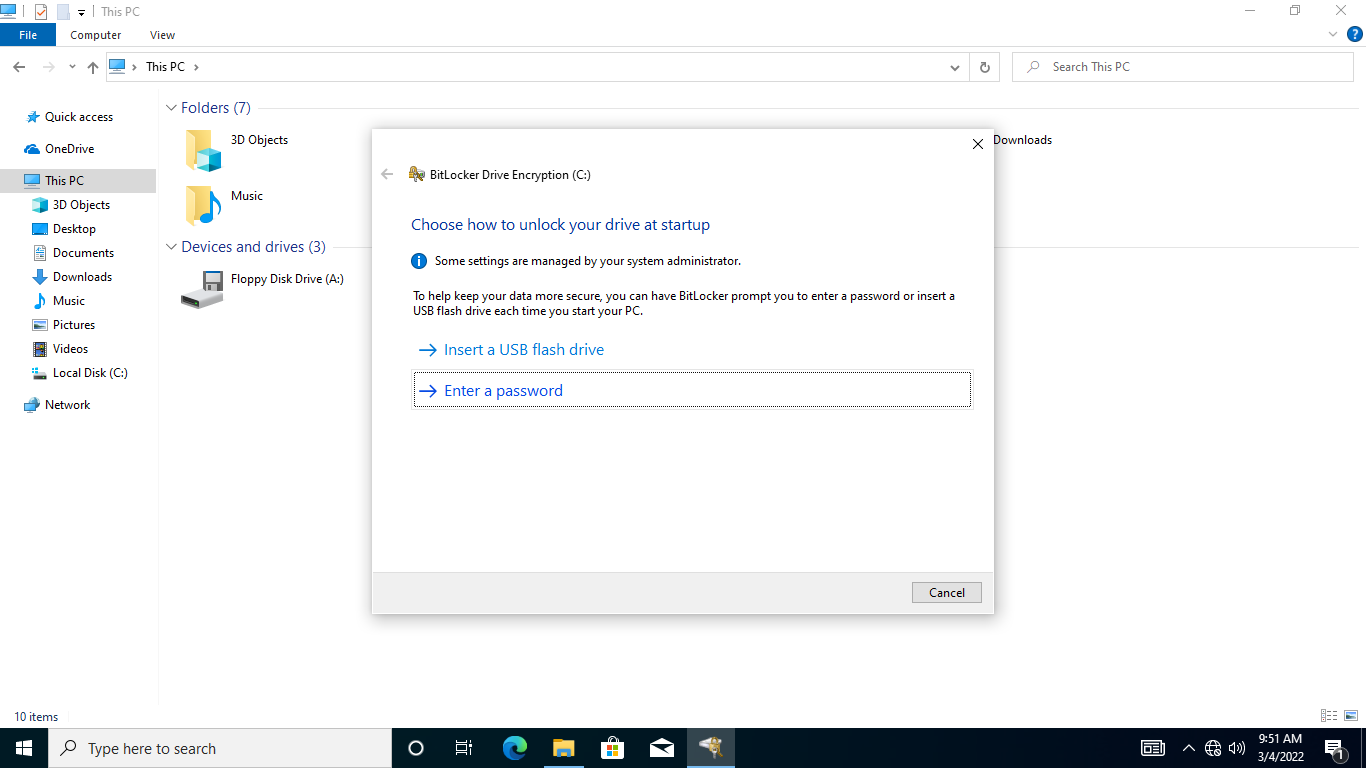
On **NTWIN10HV1** desktop, click File Explorer on the Taskbar.

Expand **This PC** and right-click **Local Disk (C:)** then select **Turn on BitLocker.**



**Step 2:**

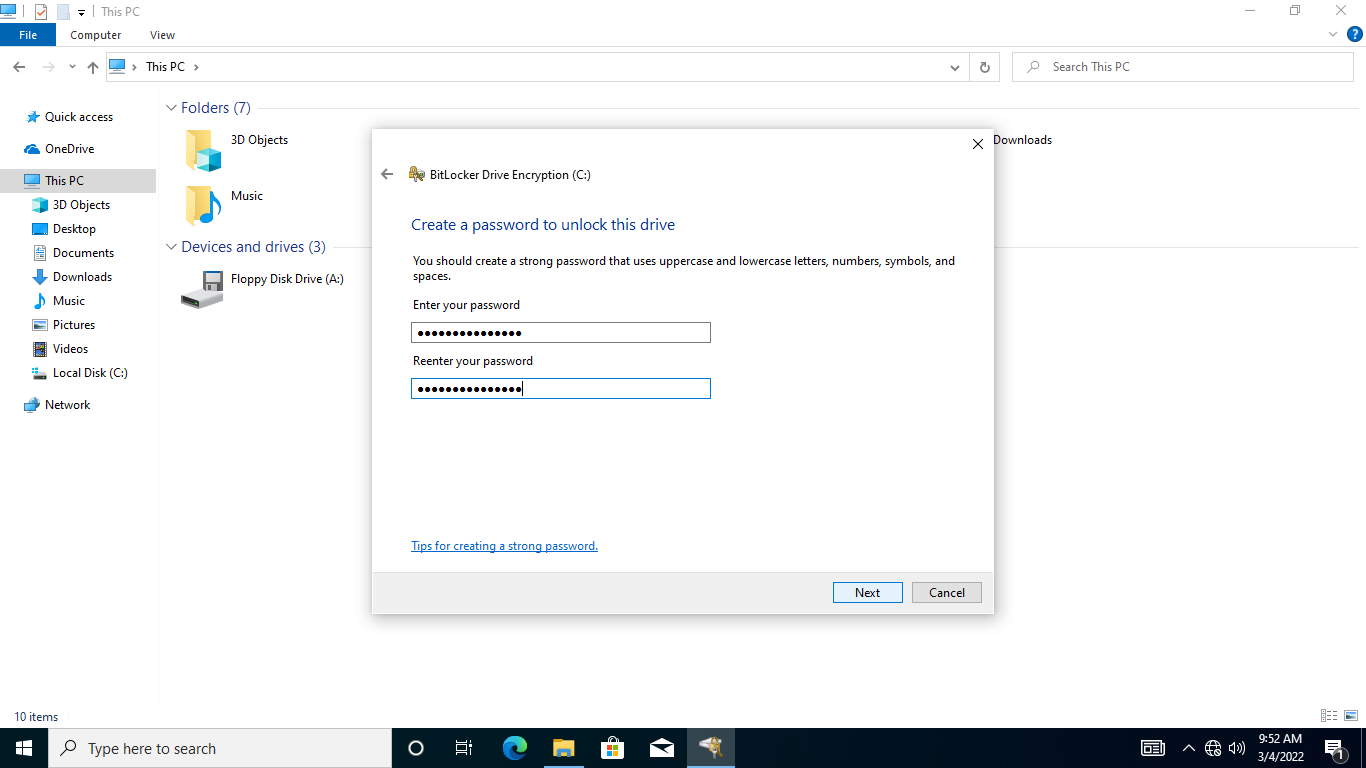
On the **BitLocker Drive Encryption (C:)** - **Choose how to unlock your drive at startup** page, select **Enter a password**



**Step 3:**

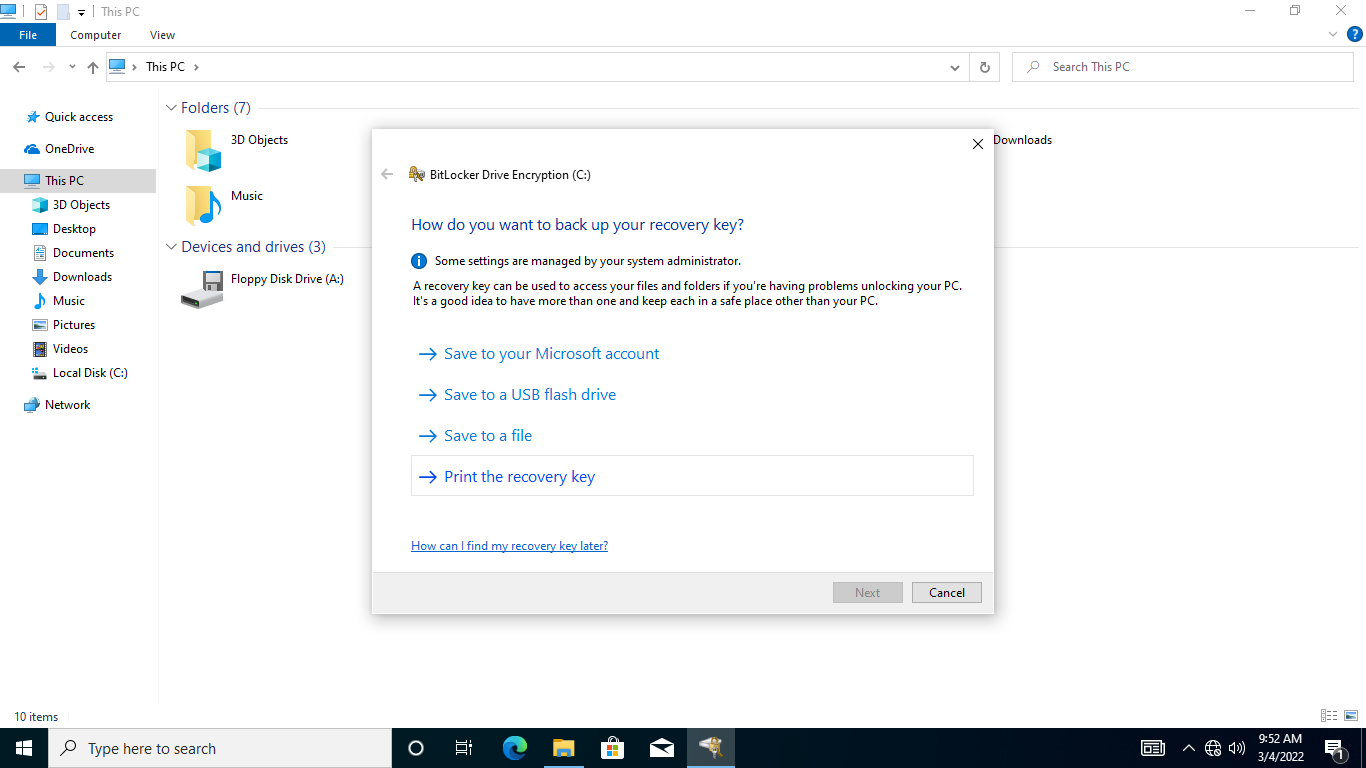
On the **Create a password to unlock this drive** page, in the **Enter your password** and **ReEnter your password** textboxes, type: ***Networktute@123***

Click **Next.**



**Step 4:**

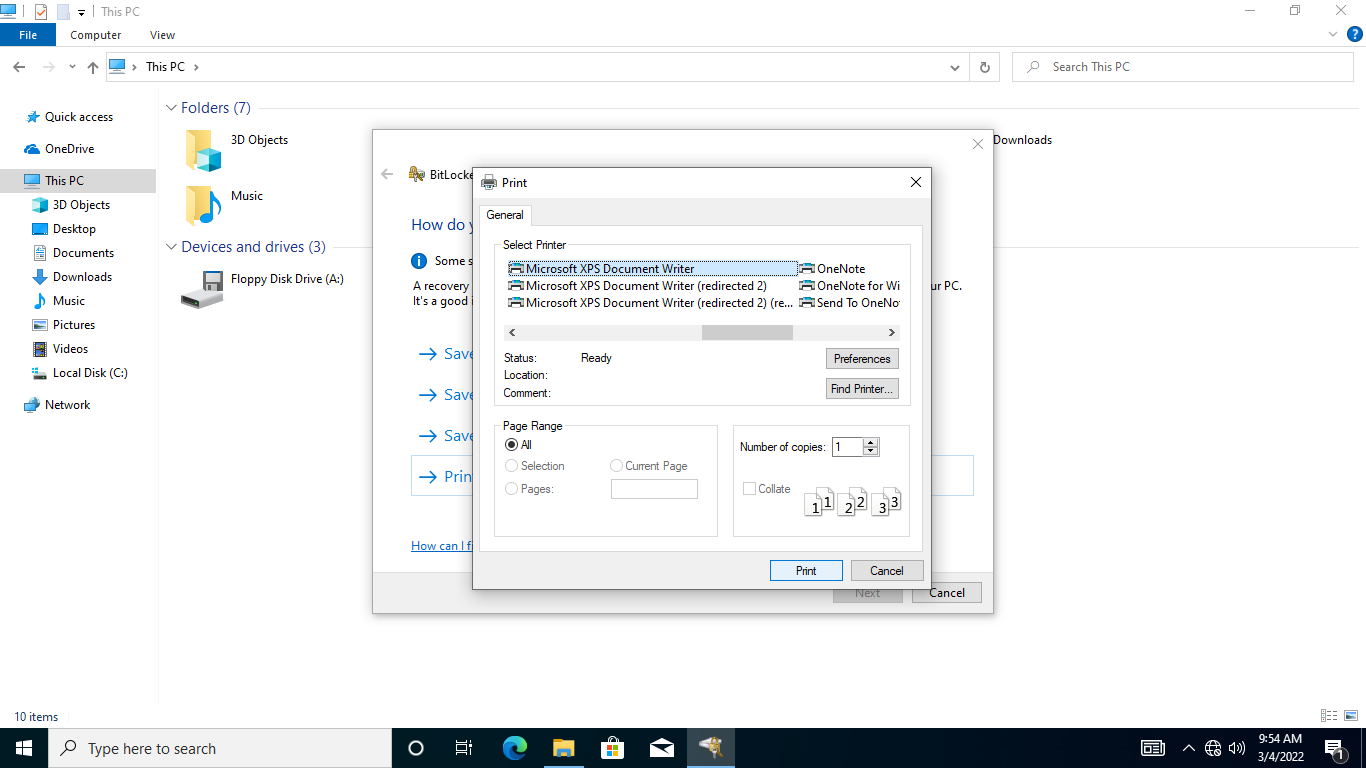
On the **How do you want to back up your recovery key** page, click **Print the recovery key**.



**Step 5:**

On the **Print** dialog box, click **Microsoft XPS Document** **Writer**.

Click **Print**.

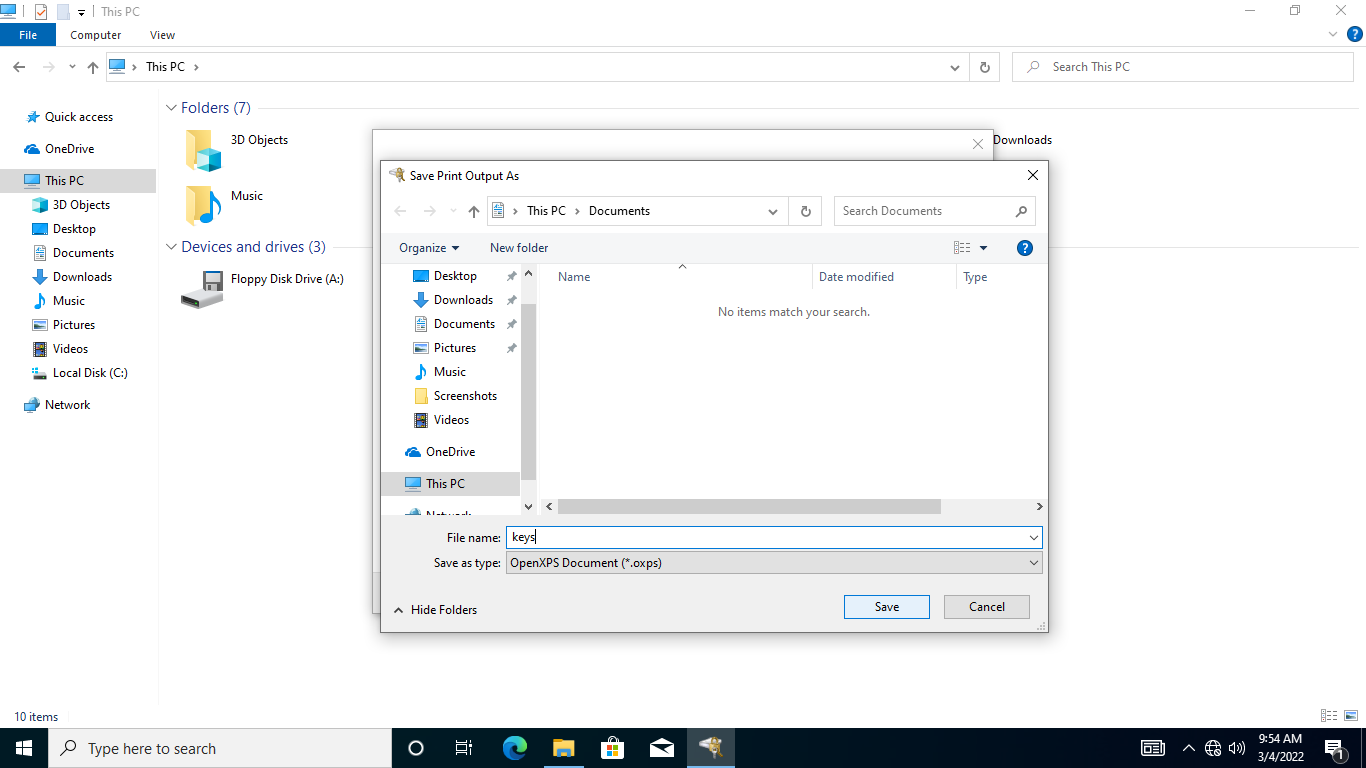


**Step 6:**

On the **Save Print Output As** dialog box, in the **File name** textbox, type: ***keys***

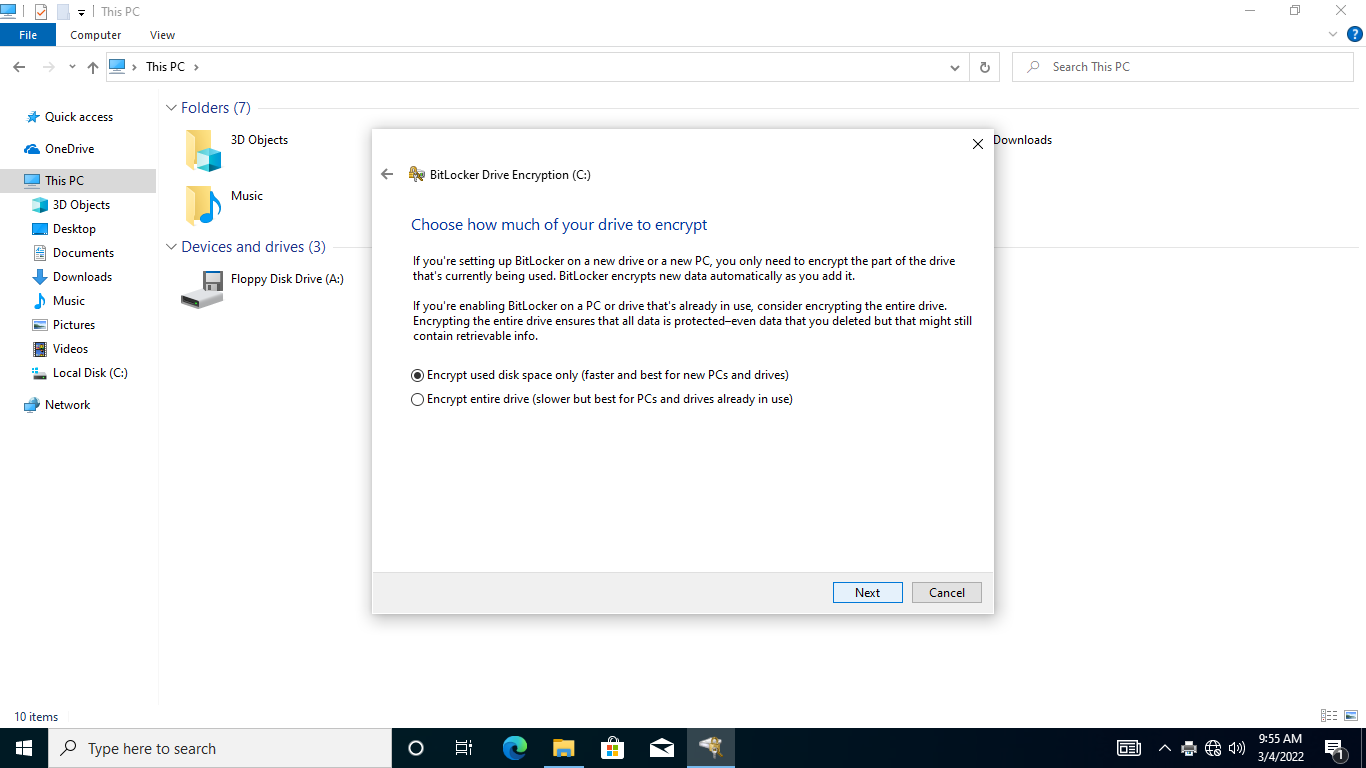
Click **Save.**

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



**Step 7:**

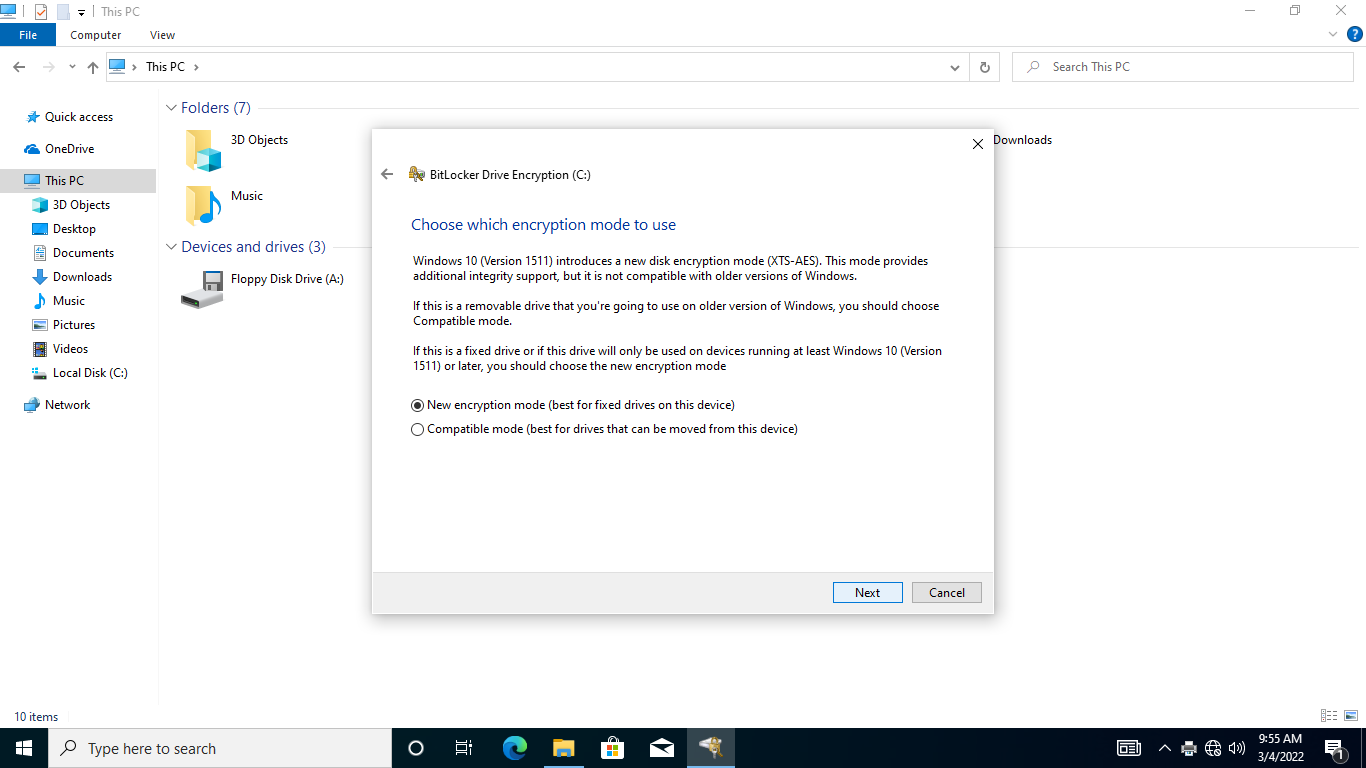
In the **Choose how much of your drive to encrypt** and keep the default settings. Click **Next**



**Step 8:**

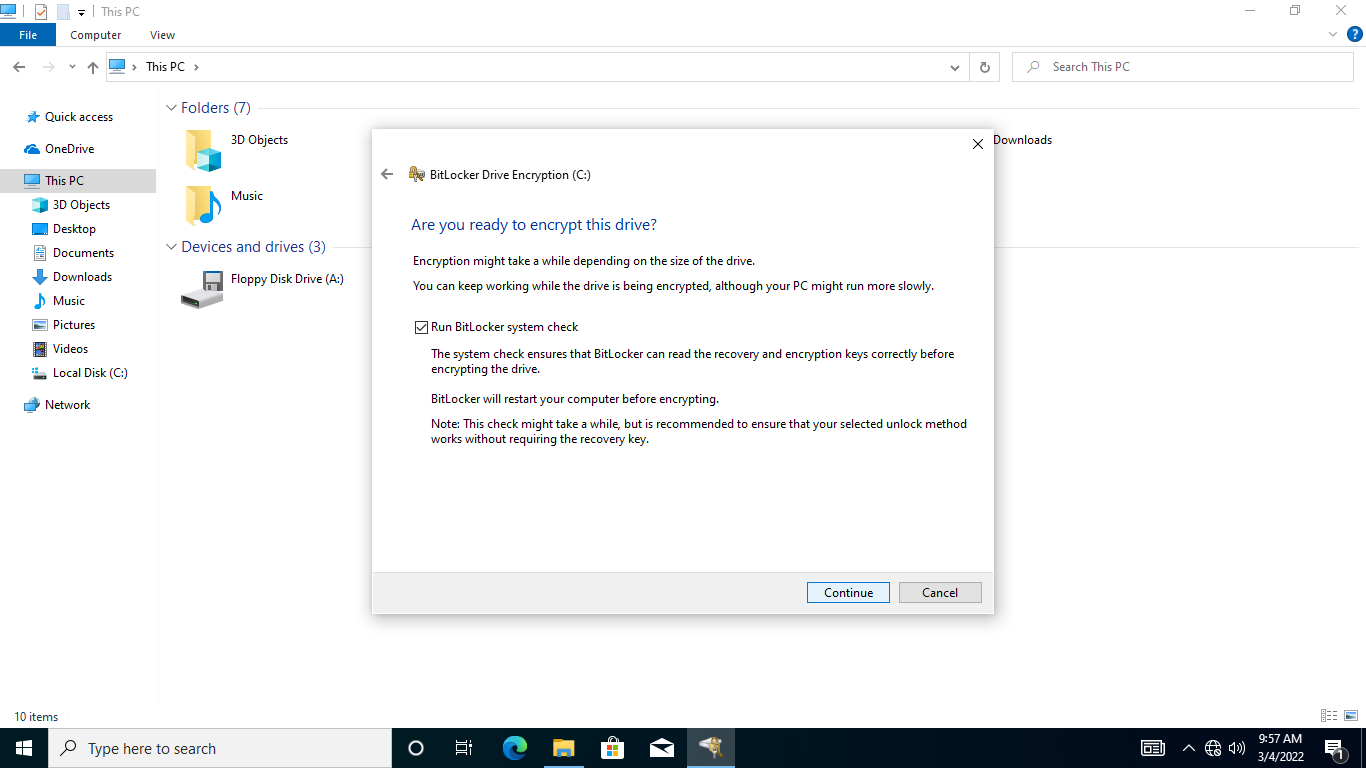
On the **Choose which encryption mode to use** page, keep the default selection.

Click **Next**.



**Step 9:**

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

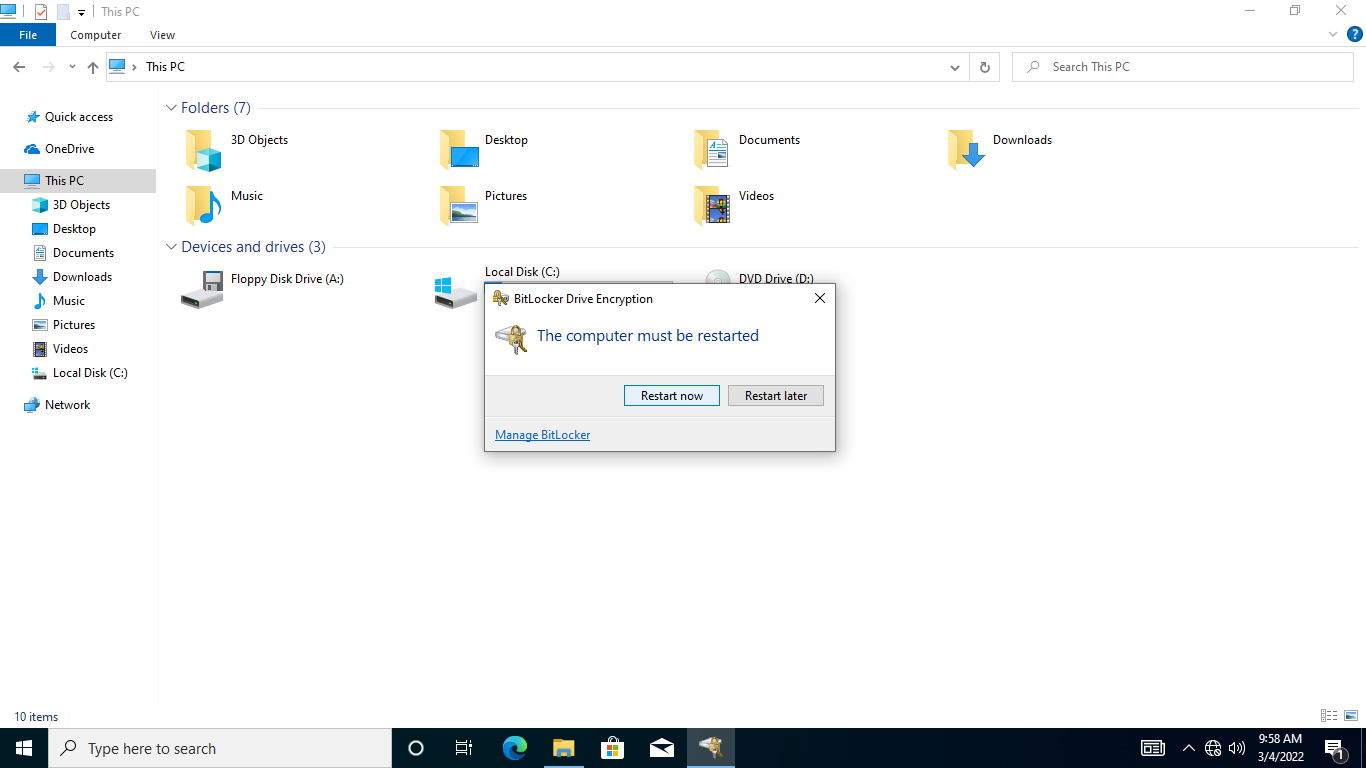


**Step 10:**

A message appears in the system tray that encryption will begin after computer restart.

In **BitLocker Drive** **Encryption**, Click **Restart Now.**

To force a restart, right-click **Start**, point to **Shut down or sign out** and select **Restart**



**Step 11:**

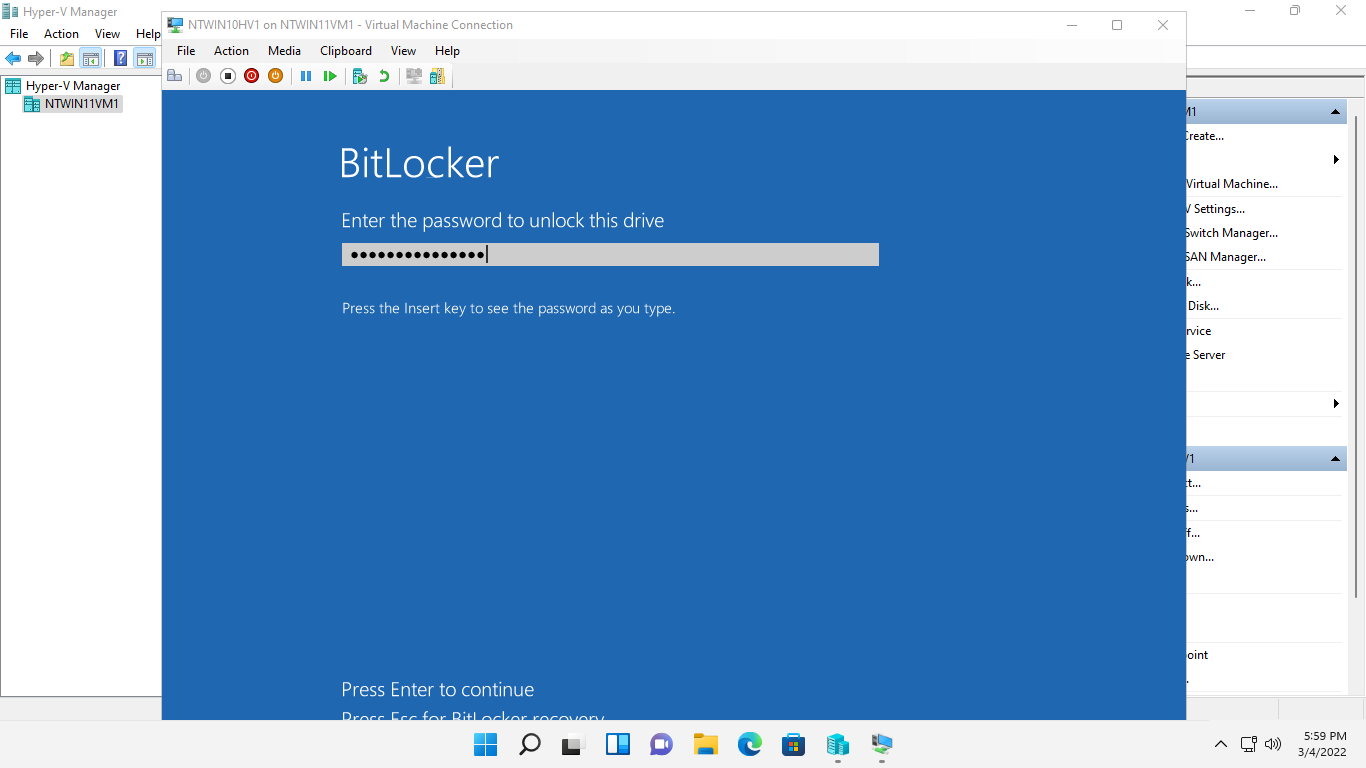
Please wait while **NTWIN10HV1** is starting up.

Notice that there is BitLocker screen that asks for the password to unlock this drive.

|  |
| --- |
| **Note**: In addition, there is BitLocker recovery key to use, in the event the password is unknown. |

In the textbox, type: ***Networktute@123***

Press **Enter**.



**Step 12:**

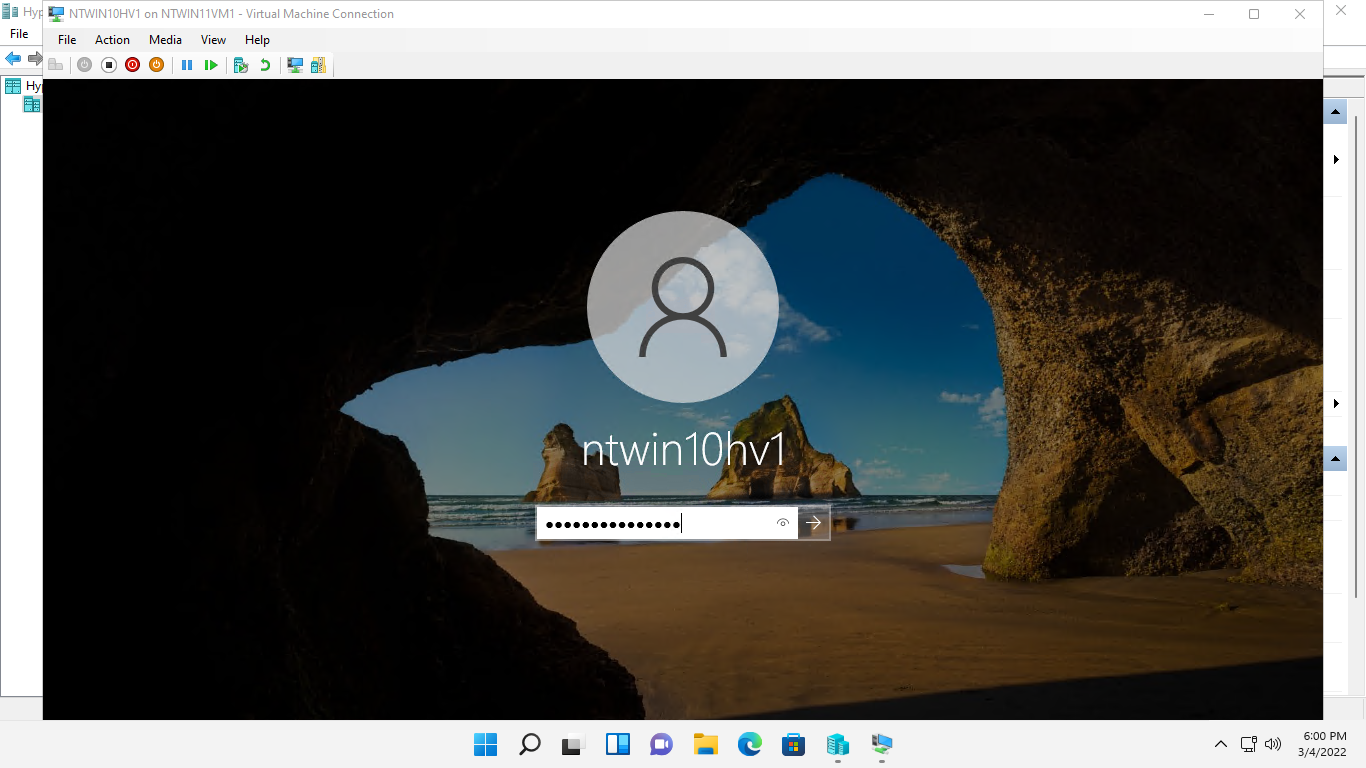
**NTWIN10HV1** continues to start up.

Then the sign-in page appears. This means that the system drive is protected from unauthorized users.

Sign-in as admin.

The password is: ***Networktute@123***

Press **Enter**.

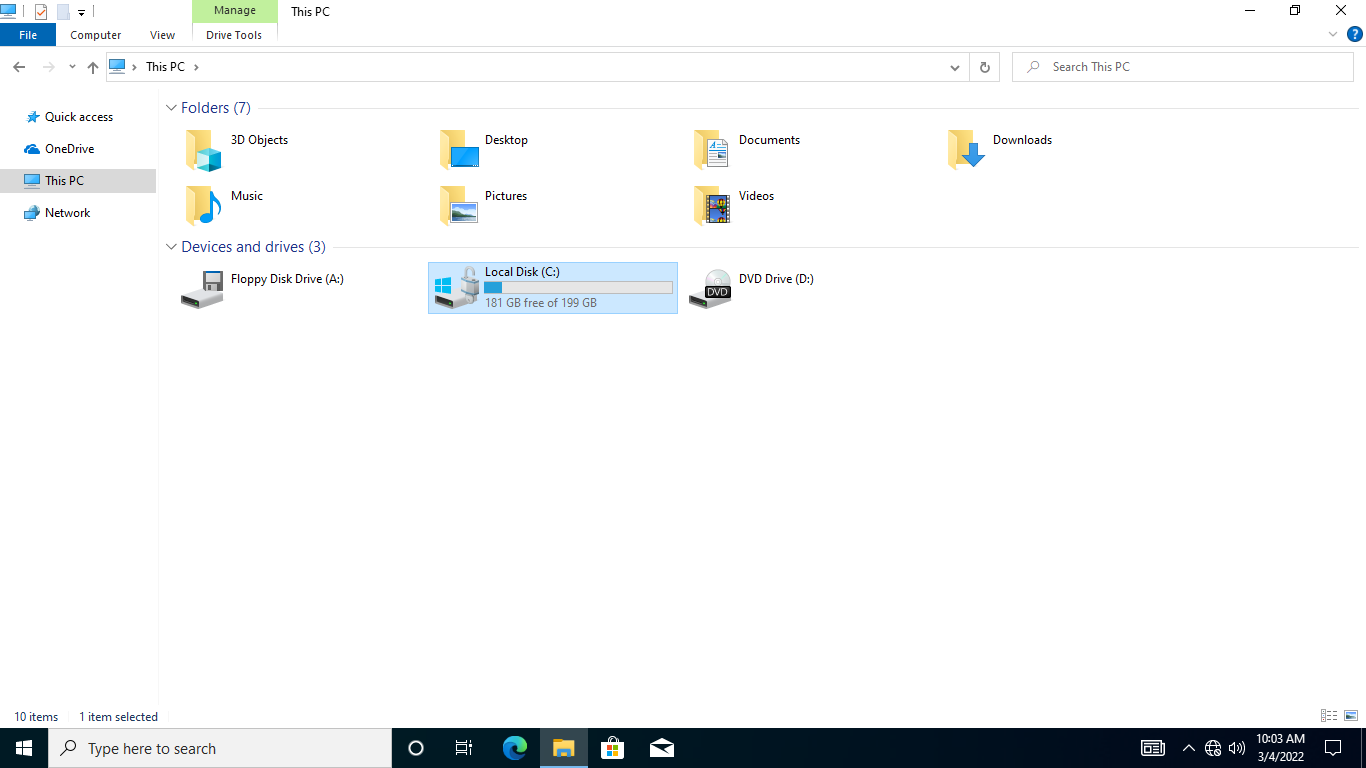


**Step 13:**

When signed-in, click **View**, then click **Full Screen Mode.**

Launch **File Explorer** from the **Taskbar.**

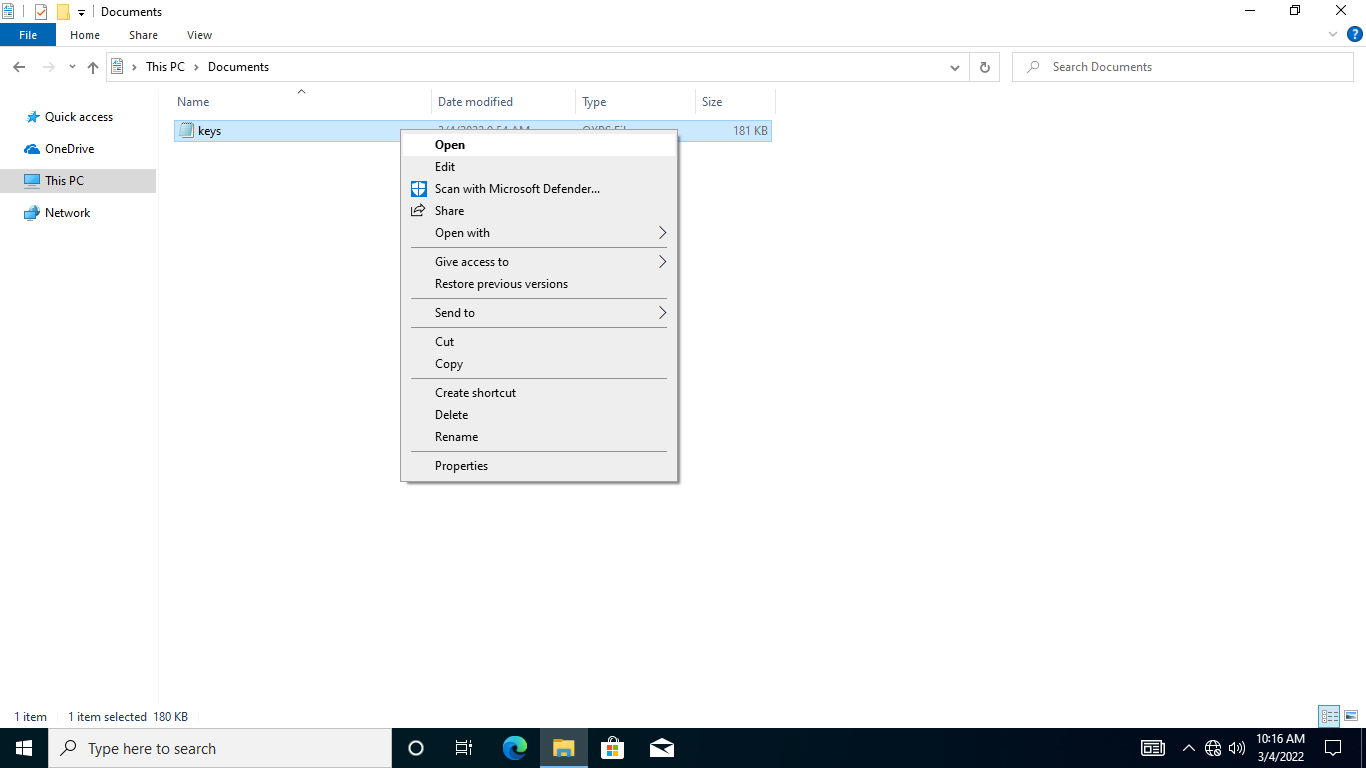
Select **This PC** node and notice the **Local Disk (C:)** drive is now unlocked because you entered the correct BitLocker password during startup



**Step 14:**

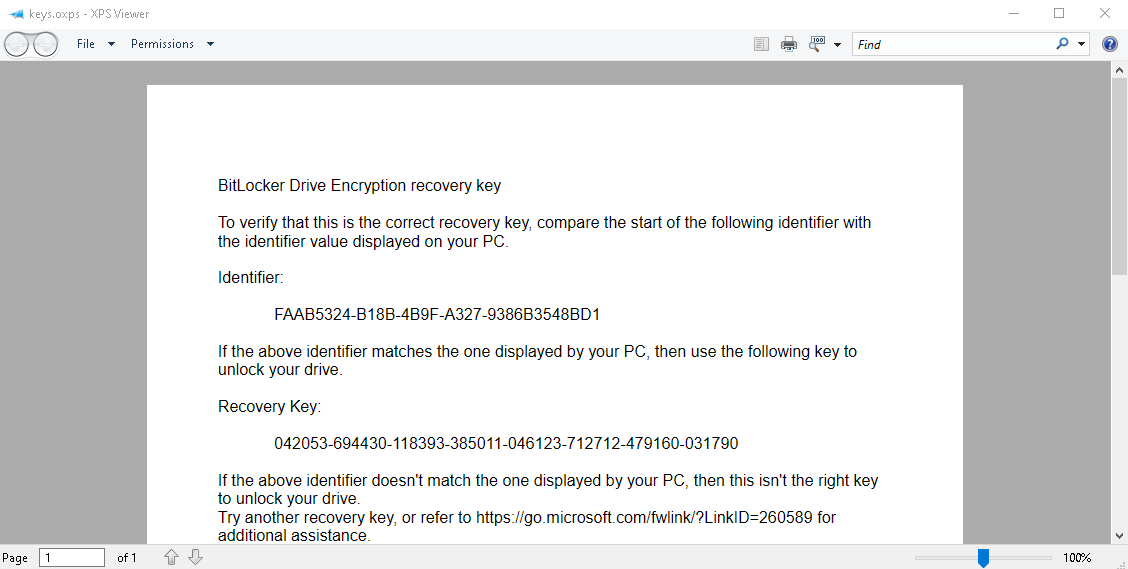
From the **File Explorer** window, navigate to **This PC > Documents** folder.

Right-click the **keys XPS** document and select **Open**.



**Step 15:**

Notice the **XPS** file shows an example of a **BitLocker Drive Encryption Recovery Key**



**Step 16:**

Close the **Keys** XPS file.

Exit from **File Explorer**.

Close the **NTWIN10HV1** guest virtual machine.

