Lab 4: Perform Disk Encryption

Lab Scenario

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Lab Objectives

- Perform disk encryption using VeraCrypt
- Perform disk encryption using BitLocker Drive Encryption
- Perform disk encryption using Rohos Disk Encryption

Overview of Disk Encryption

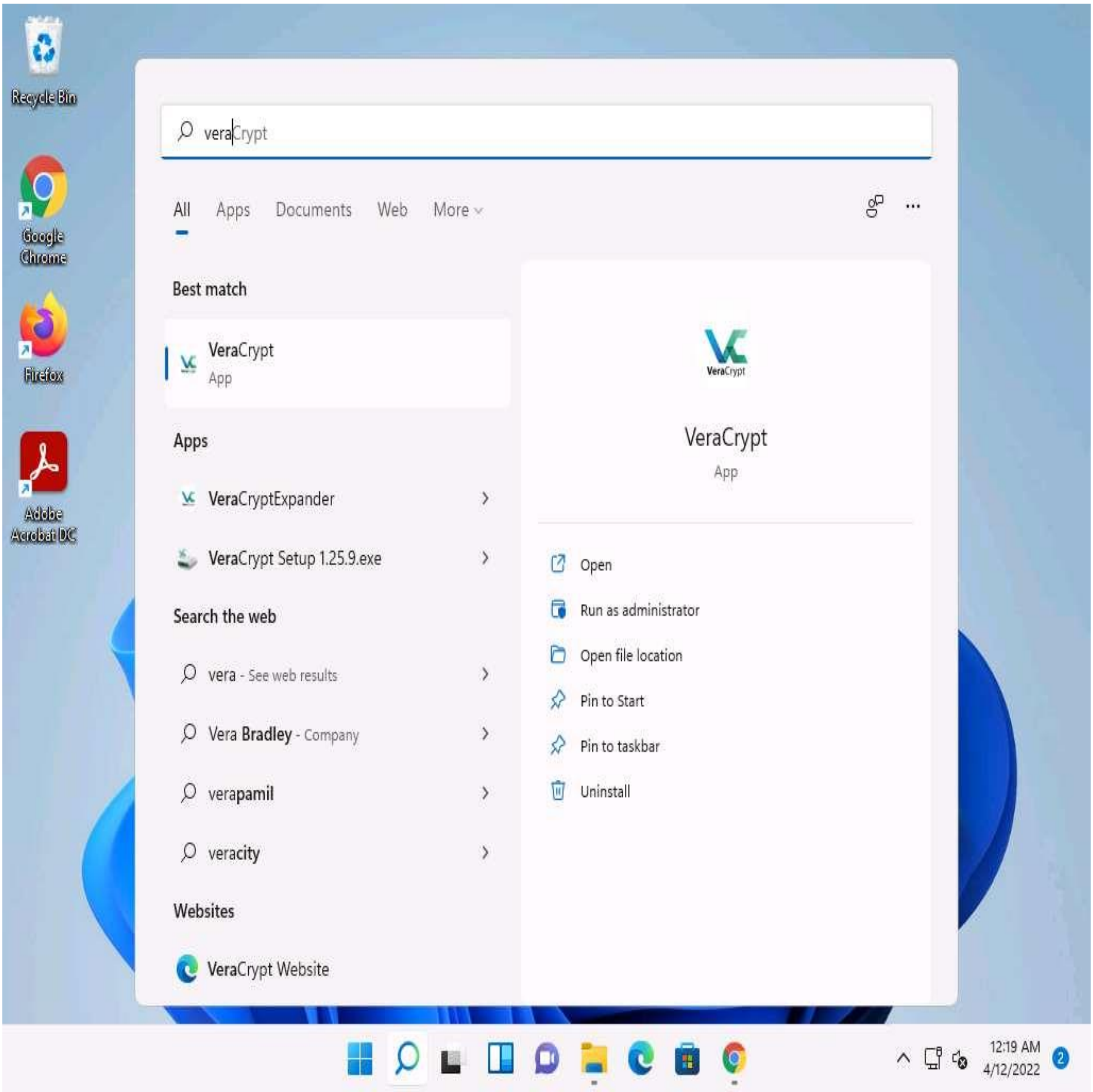
Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Task 1: Perform Disk Encryption using VeraCrypt

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

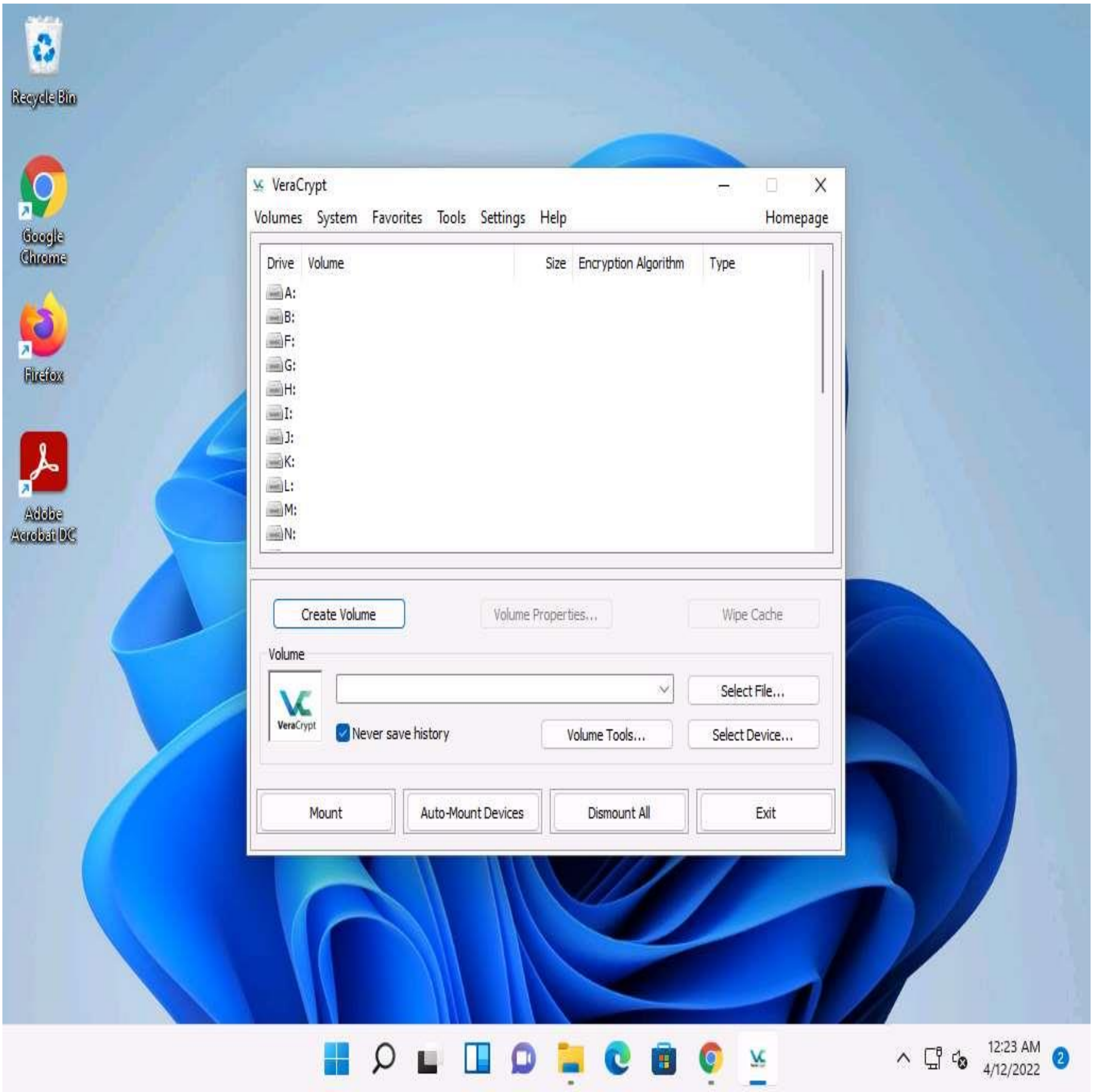
Here, we will use the VeraCrypt tool to perform disk encryption.

1. □ Click Windows 11 to switch to the **Windows 11** machine.
2. □ Click **Search** icon (🔍) on the **Desktop**. Type **vera** in the search field, the **VeraCrypt** appears in the results, click **Open** to launch it.

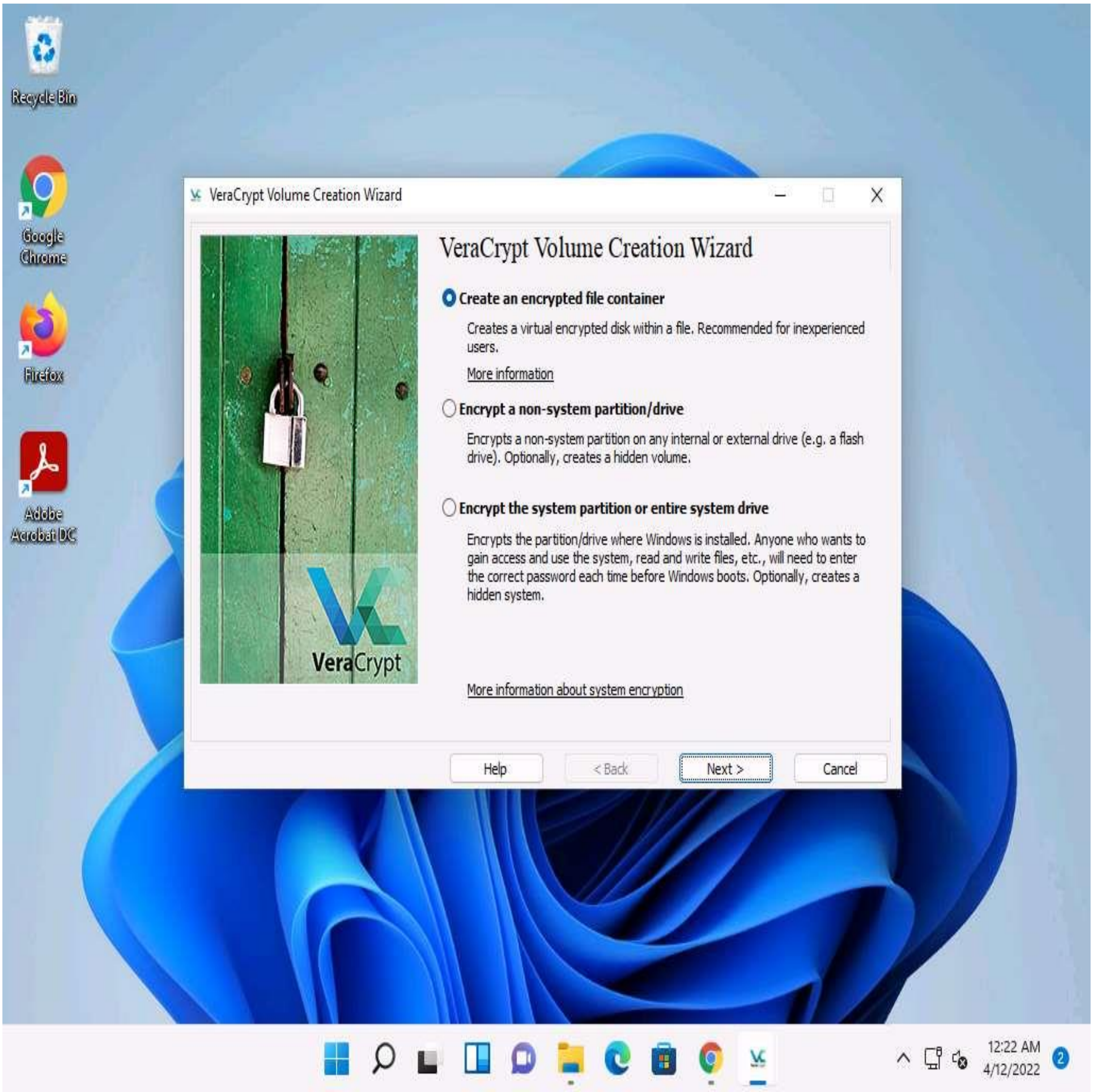


veraCrypt

3. ☐ The **VeraCrypt** main window appears; click the **Create Volume** button.



4. □ The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.



VeraCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Encrypt a non-system partition/drive

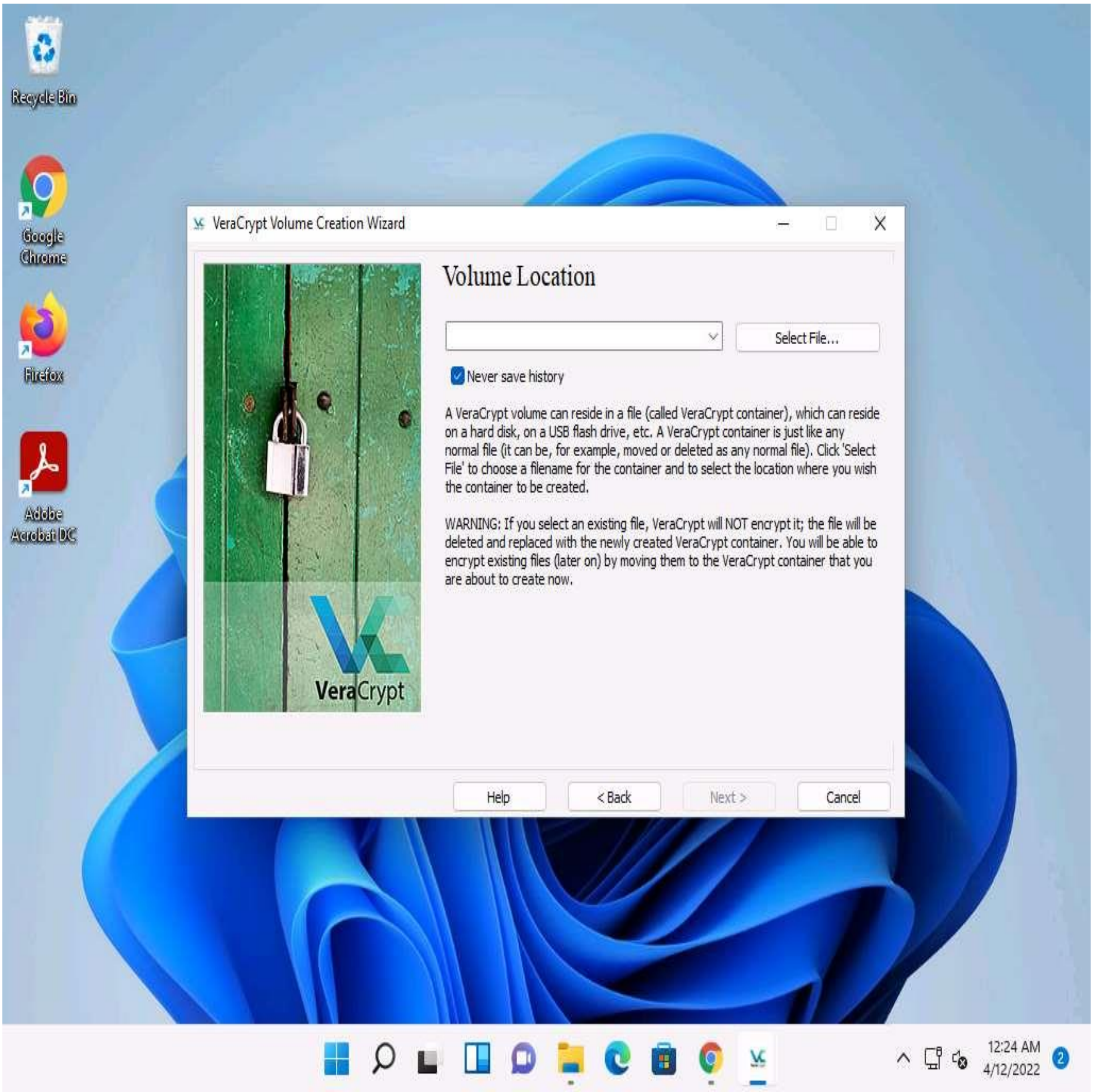
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

5. □ In the **Volume Type** wizard, keep the default settings and click **Next**.
6. □ In the **Volume Location** wizard, click **Select File...**.



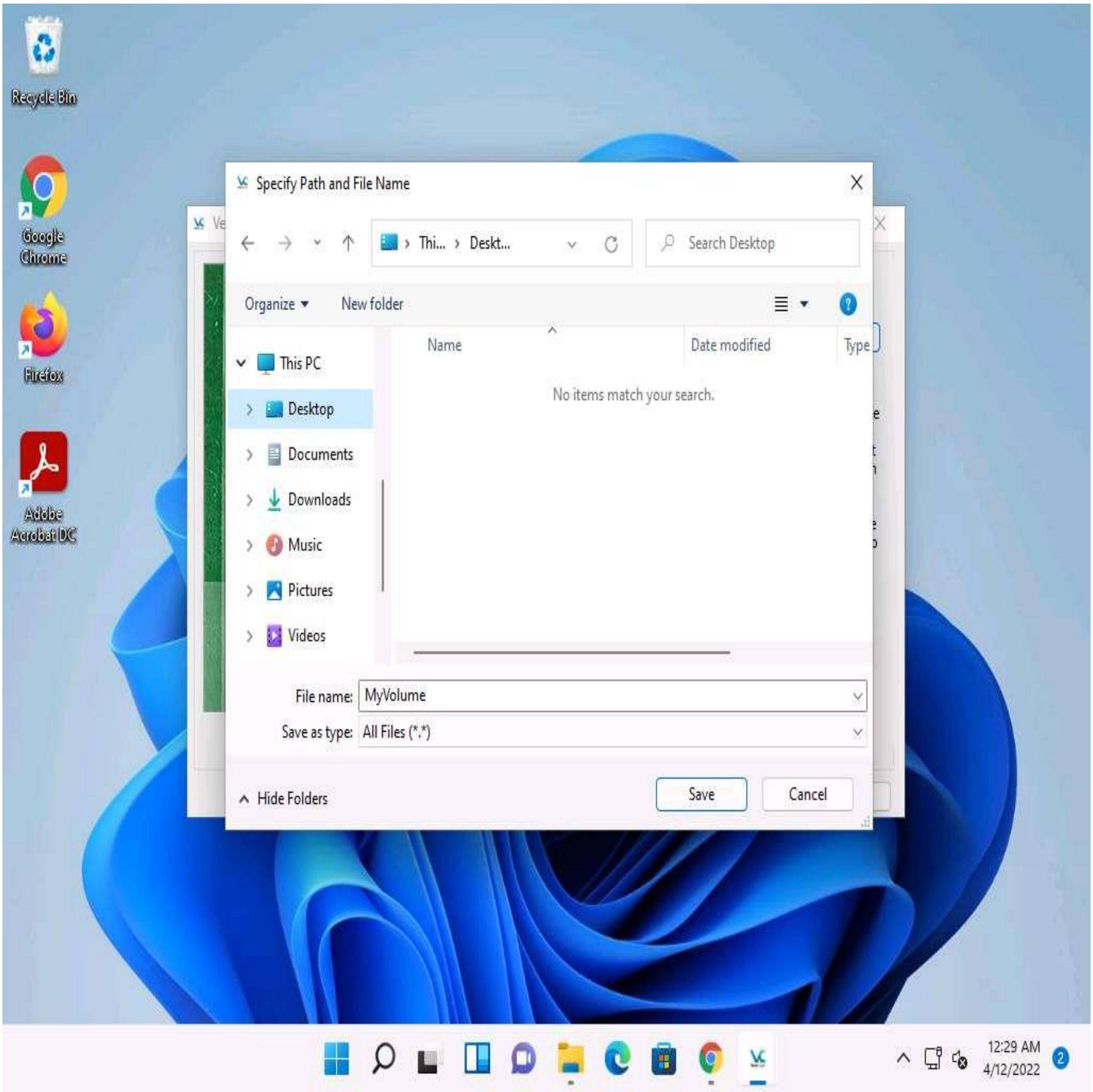
Volume Location

☑ Never save history

A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

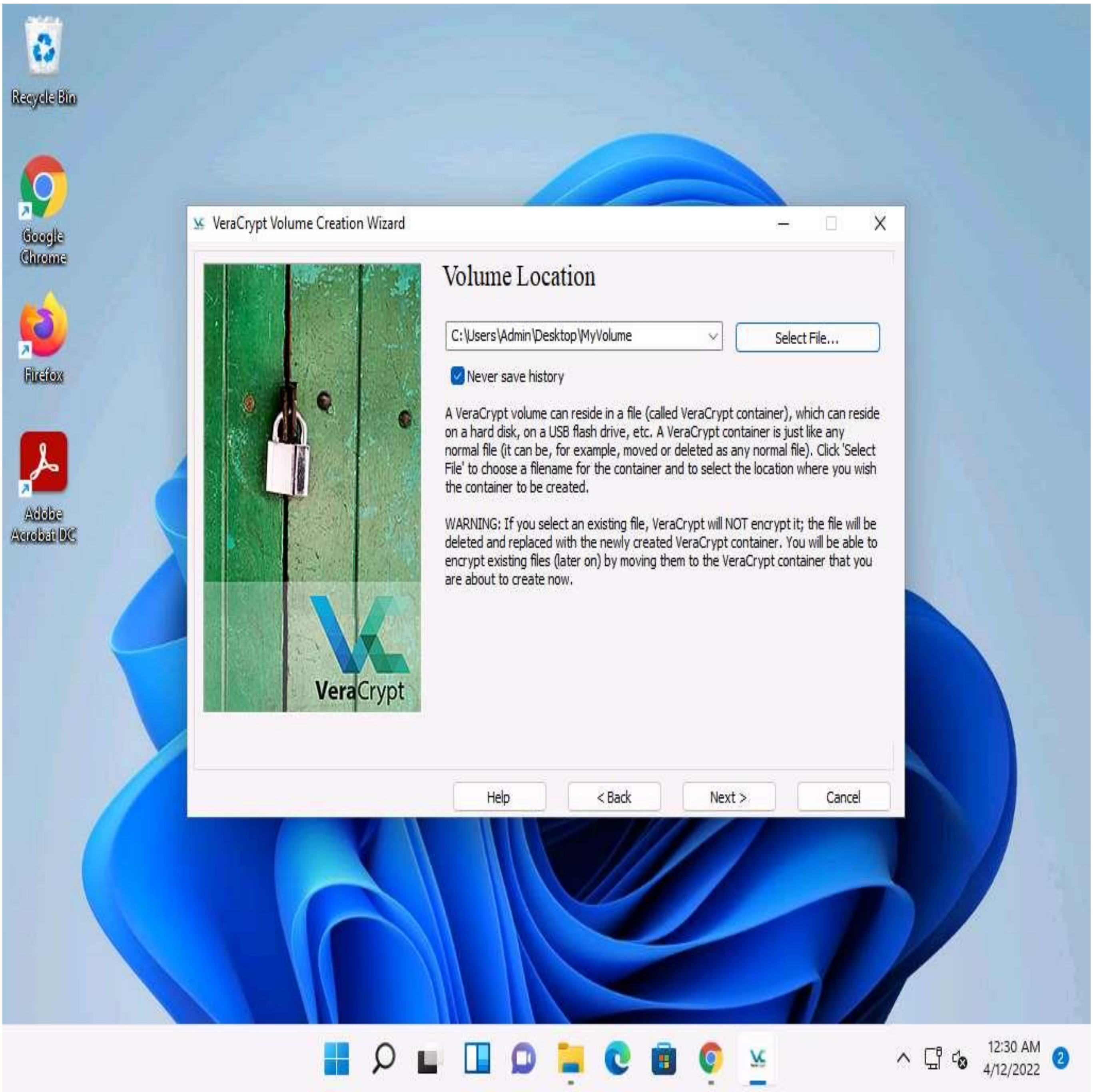
7. □ The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **MyVolume**, and click **Save**.



File name: MyVolume

Save as type: All Files (*.*)

8. □ After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.



Volume Location

C:\Users\Admin\Desktop\MyVolume

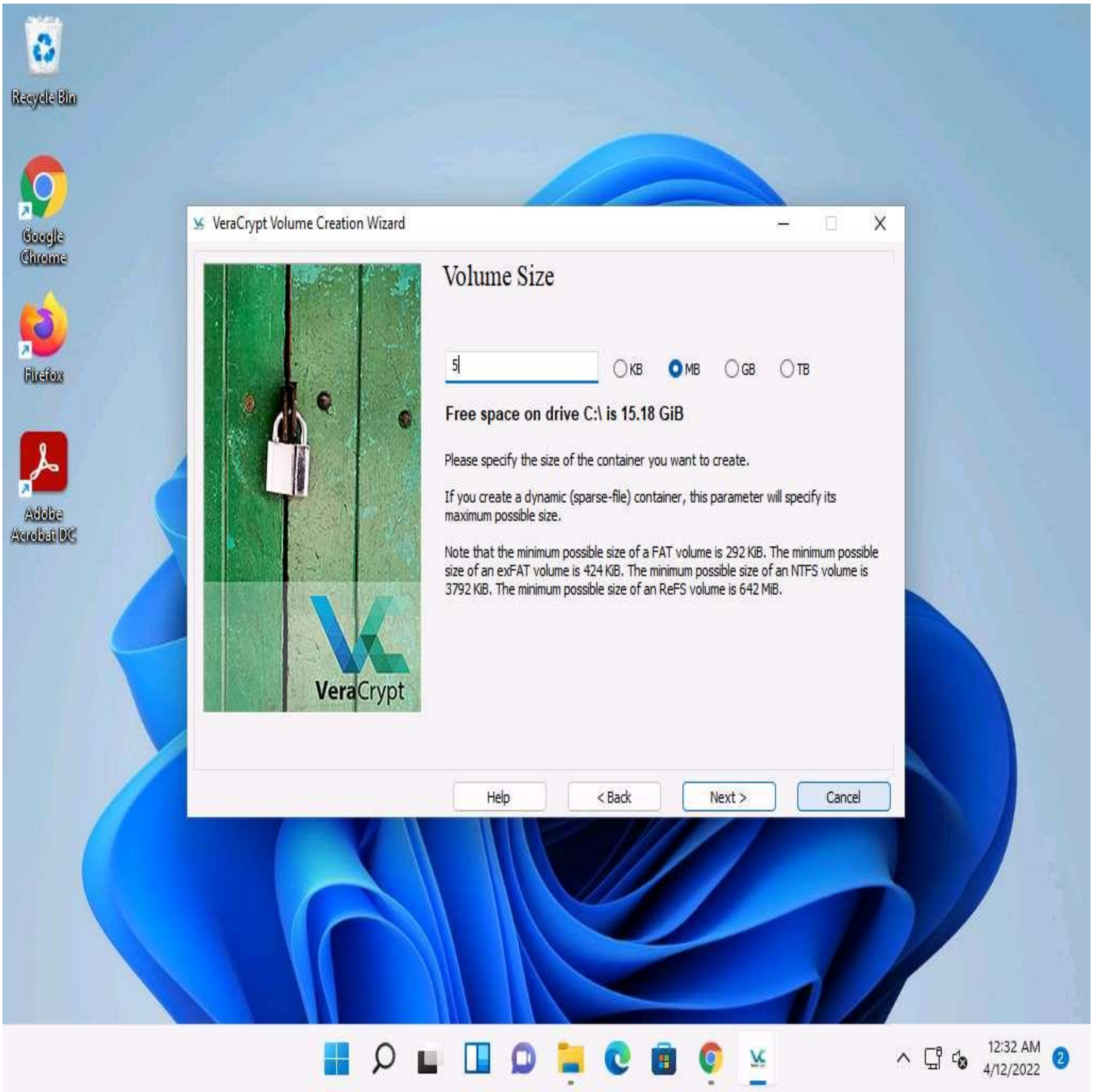
☑ Never save history

A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

9. □ In the **Encryption Options** wizard, keep the default settings and click **Next**.

10. □ In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.



VeraCrypt Volume Creation Wizard

Volume Size

5 ○ KB ● MB ○ GB ○ TB

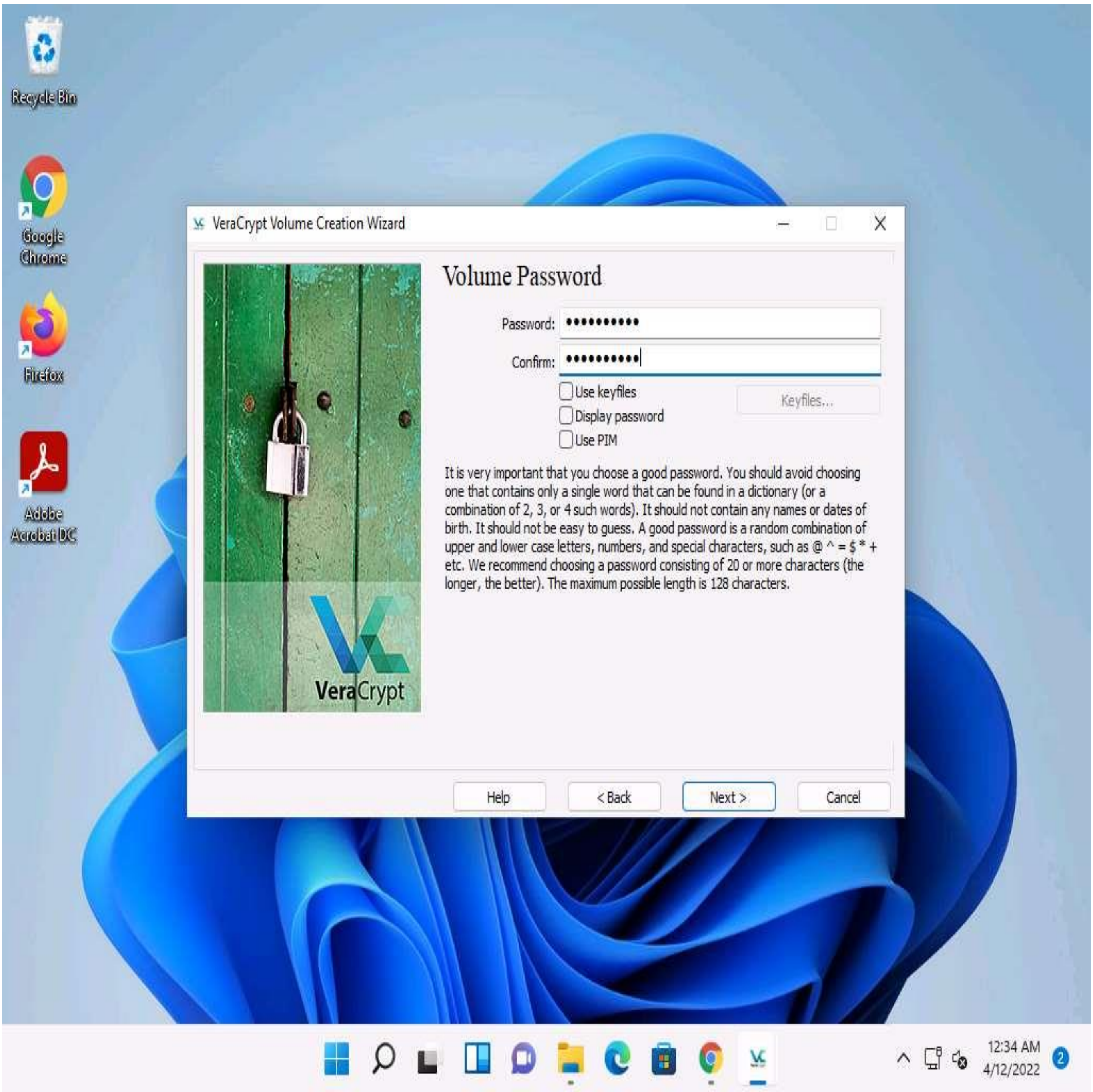
Free space on drive C:\ is 15.18 GiB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KiB. The minimum possible size of an exFAT volume is 424 KiB. The minimum possible size of an NTFS volume is 3792 KiB. The minimum possible size of an ReFS volume is 642 MiB.

11. □ The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.



VeraCrypt Volume Creation Wizard

Volume Password

Password: ••••••••••

Confirm: ••••••••••

□ Use keyfiles

□ Display password

□ Use PIM

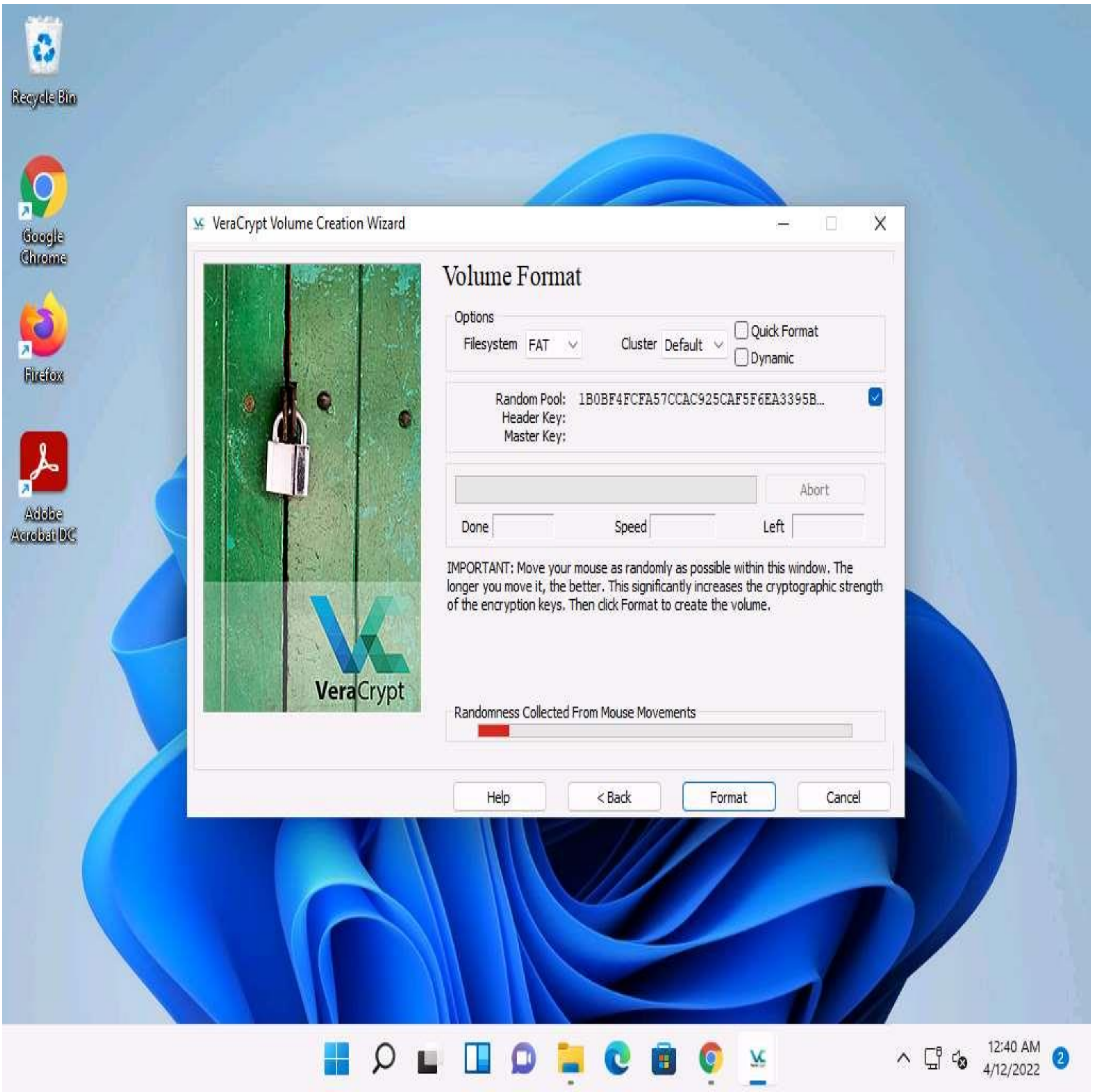
Keyfiles...

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

Help | < Back | Next > | Cancel

A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

12. □ The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.
13. □ Check the checkbox under the **Random Pool, Header Key**, and **Master Key** section.
14. □ Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.



Volume Format

Options

Filesystem FAT Cluster Default □ Quick Format □ Dynamic

Random Pool: 1B0BF4FCFA57CCAC925CAF5F6EA3395B... ☑

Header Key:

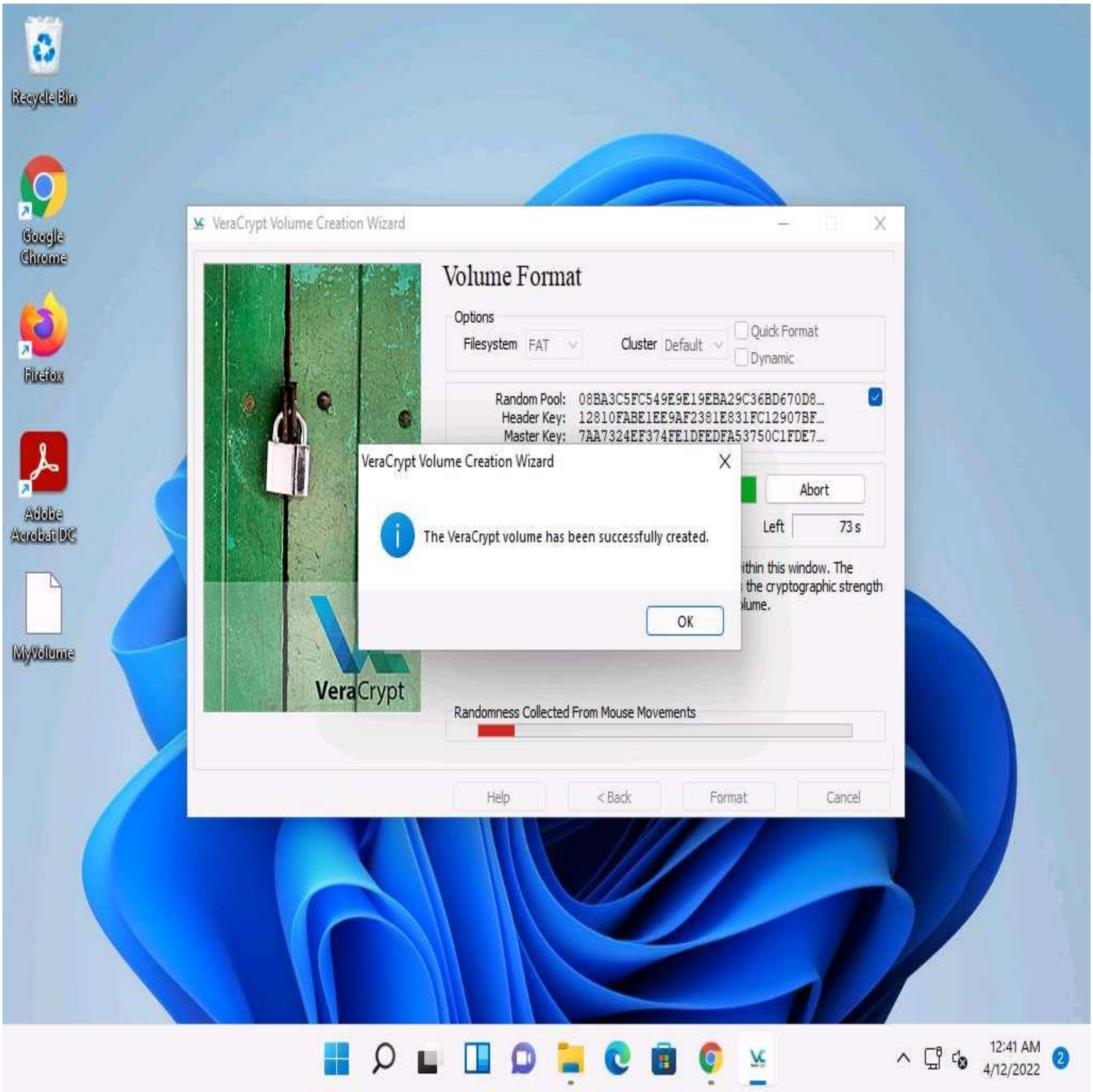
Master Key:

Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

15. □ After clicking **Format**, VeraCrypt will create a file called **MyVolume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).
16. □ Depending on the size of the volume, volume creation may take some time.
17. □ Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.



Volume Format

Options

Filesystem FAT Cluster Default □ Quick Format □ Dynamic

Random Pool: 08BA3C5FC549E9E19EBA29C36BD670D8...

Header Key: 12810FABE1EE9AF2381E831FC12907BF...

Master Key: 7AA7324EF374FE1DFEDFA53750C1FDE7...

Left 73 s

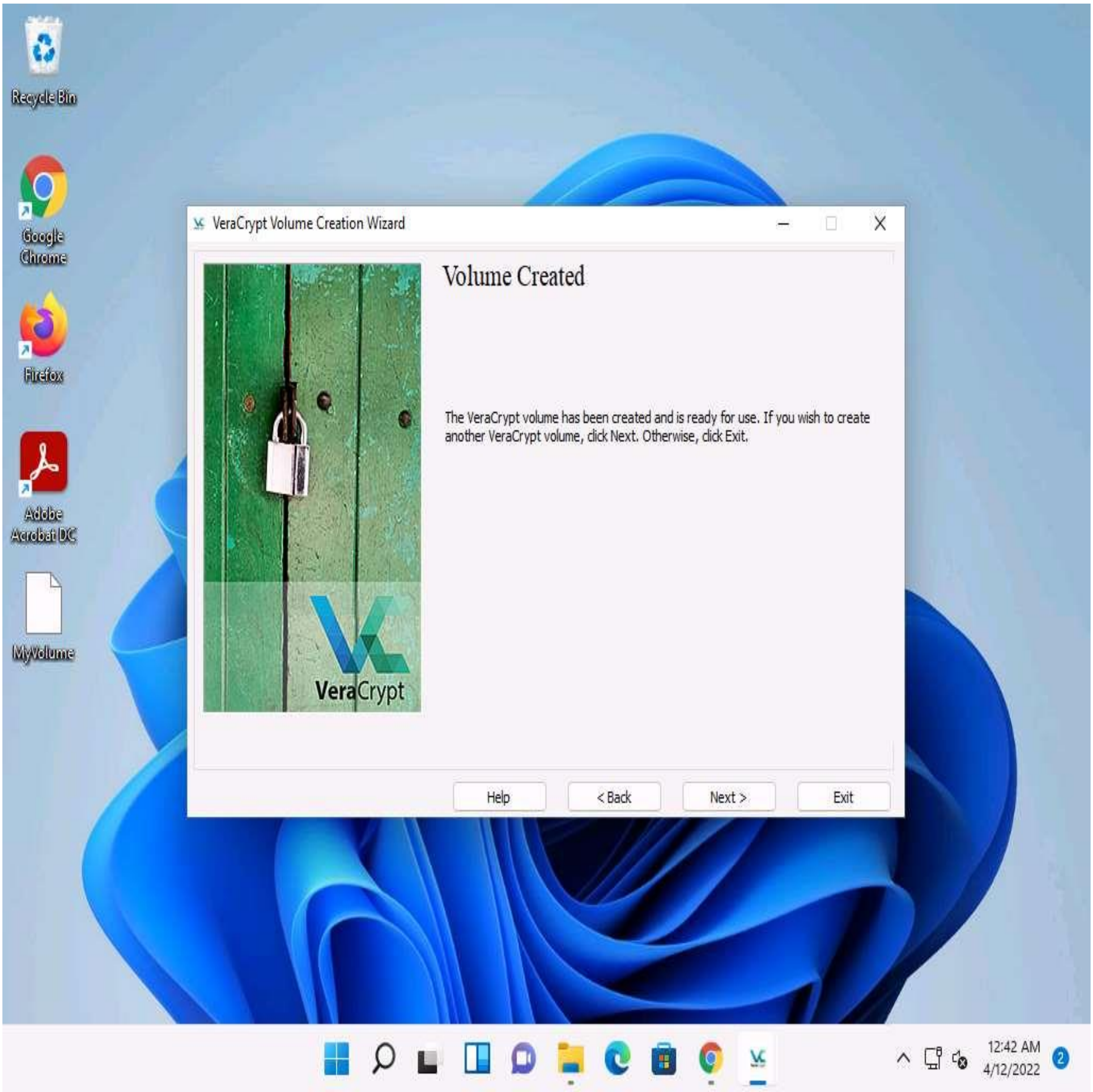
ithin this window. The the cryptographic strength lume.

Randomness Collected From Mouse Movements

VeraCrypt Volume Creation Wizard

The VeraCrypt volume has been successfully created.

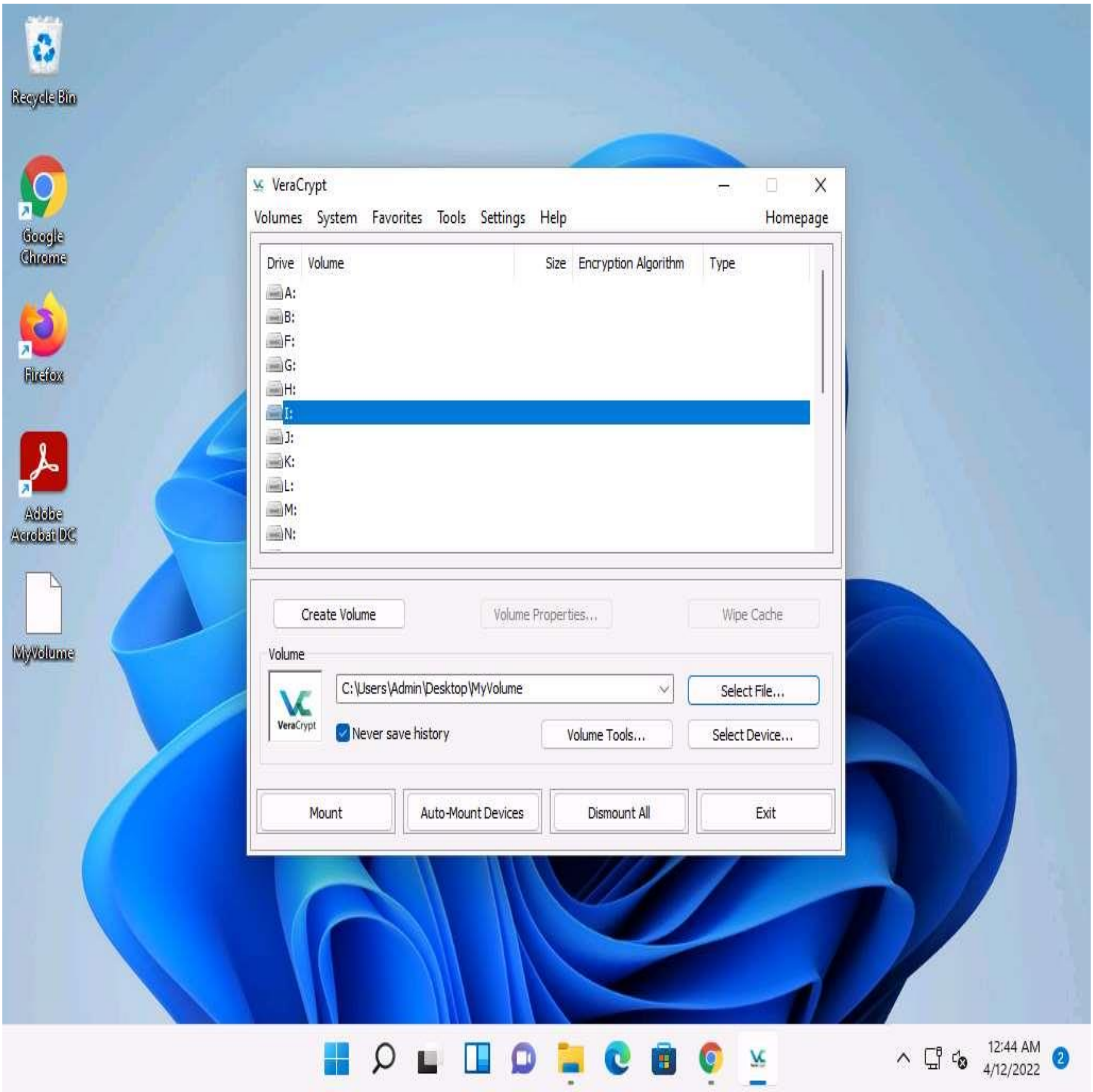
18. □ In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.



Volume Created

The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.

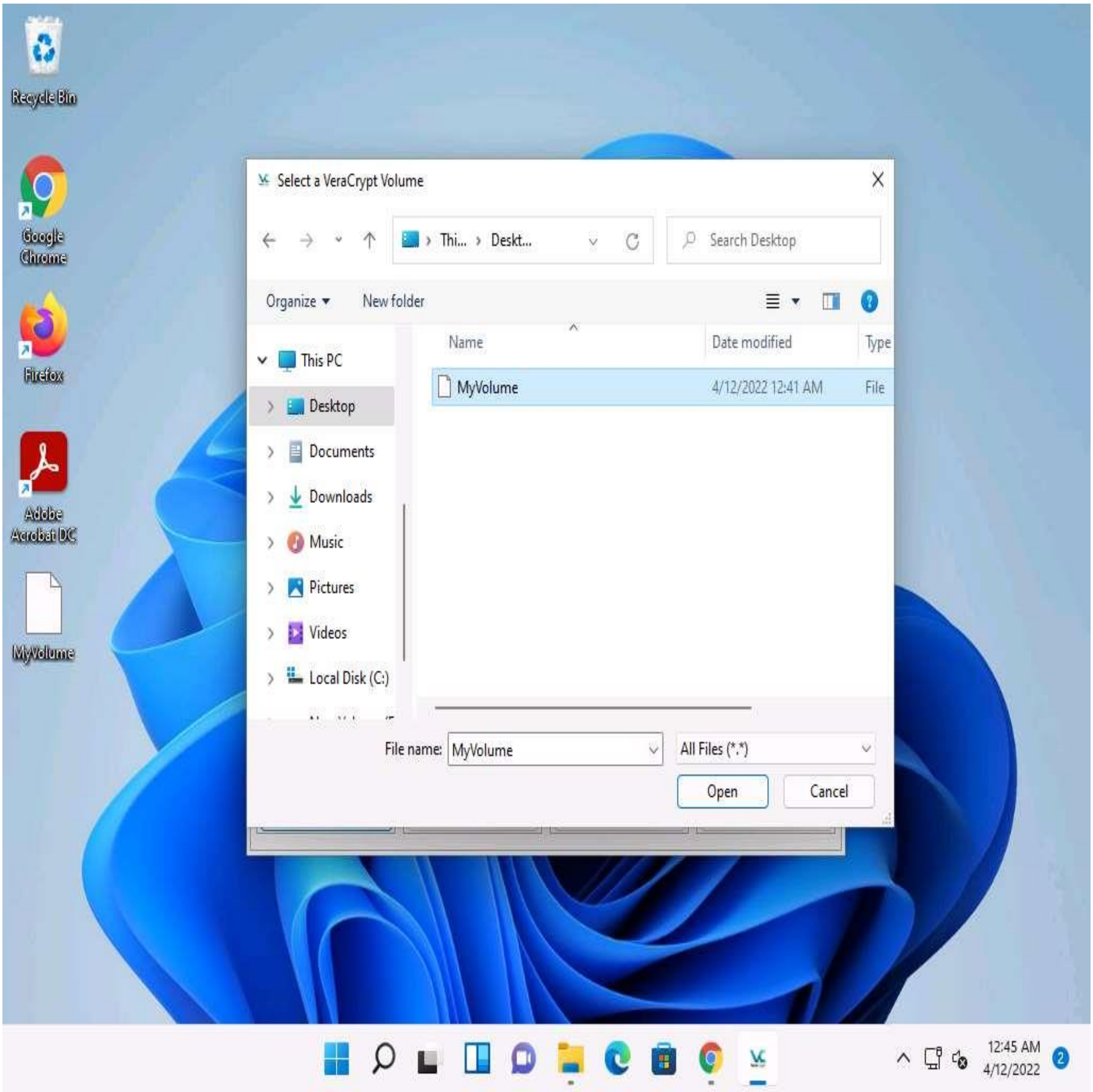
19. □ The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File...**.



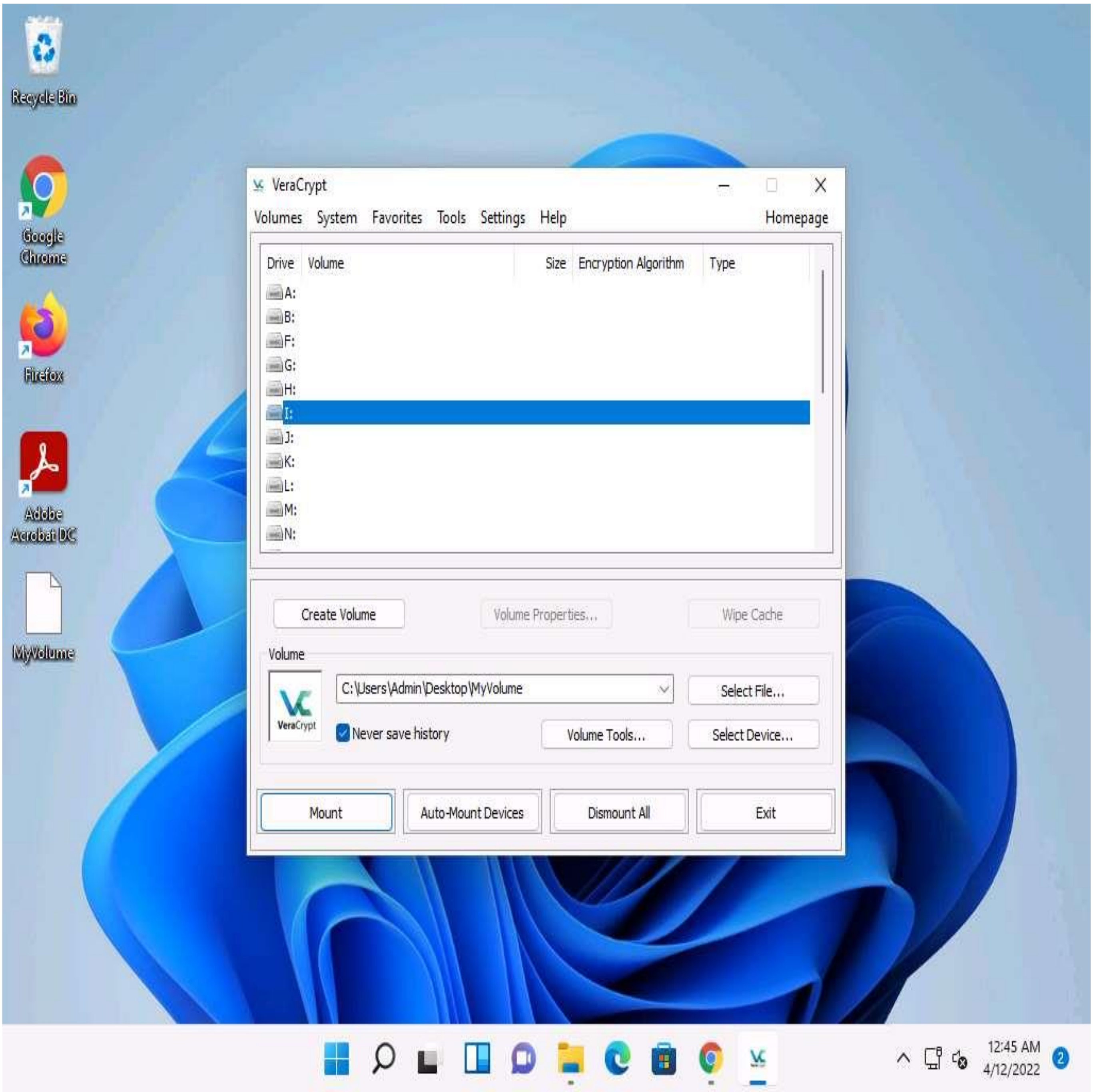
Volume: C:\Users\Admin\Desktop\MyVolume

☑ Never save history

20. □ The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **MyVolume**, and click **Open**.



21. □ The window closes, and the **VeraCrypt** window appears displaying the location of selected **volume** under the Volume field; then, click **Mount**.

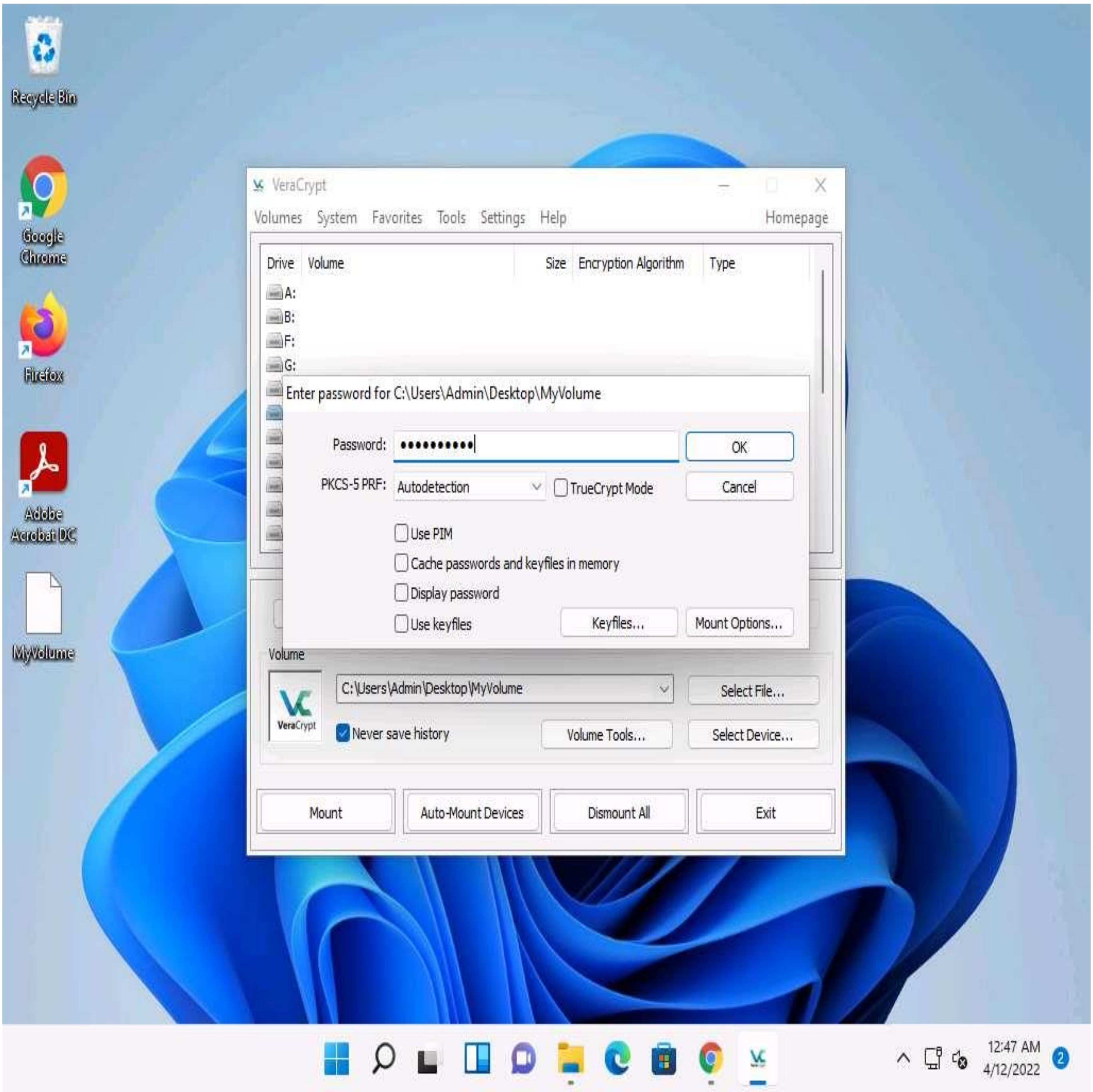


Volume: C:\Users\Admin\Desktop\MyVolume

☑ Never save history

22. □ The **Enter password** dialog-box appears; type the password you specified in **Step#11** into the **Password** field and click **OK**.

The password specified in this task is **qwerty@123**.



Enter password for C:\Users\Admin\Desktop\MyVolume

Password: ••••••••••

PKCS-5 PRF: Autodetection

□ TrueCrypt Mode

OK

Cancel

□ Use PIM

□ Cache passwords and keyfiles in memory

□ Display password

□ Use keyfiles

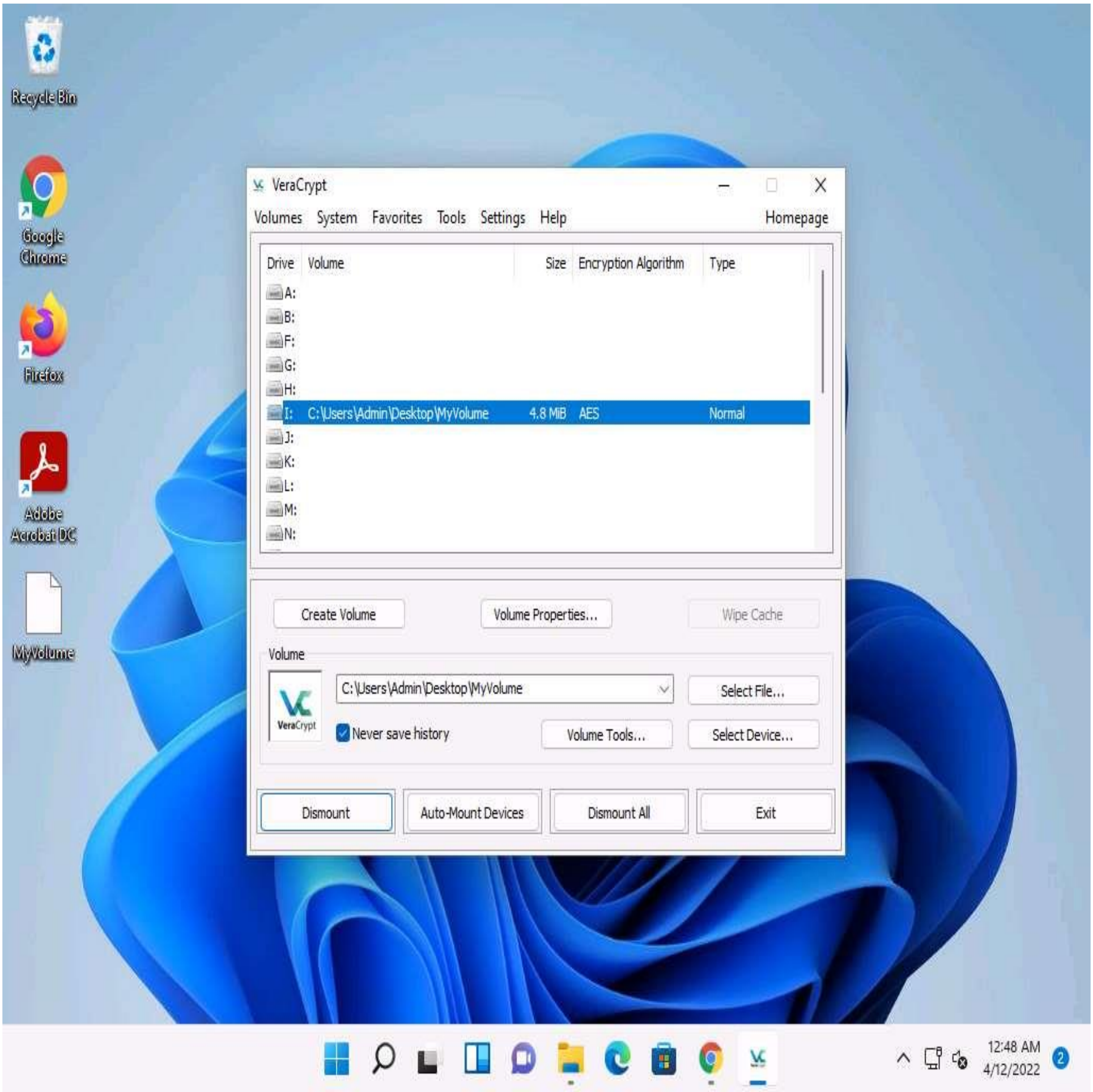
Keyfiles...

Mount Options...

C:\Users\Admin\Desktop\MyVolume

☑ Never save history

23. □ After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot:



Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
F:				
G:				
H:				
I:	C:\Users\Admin\Desktop\MyVolume	4.8 MiB	AES	Normal
J:				
K:				
L:				
M:				
N:				

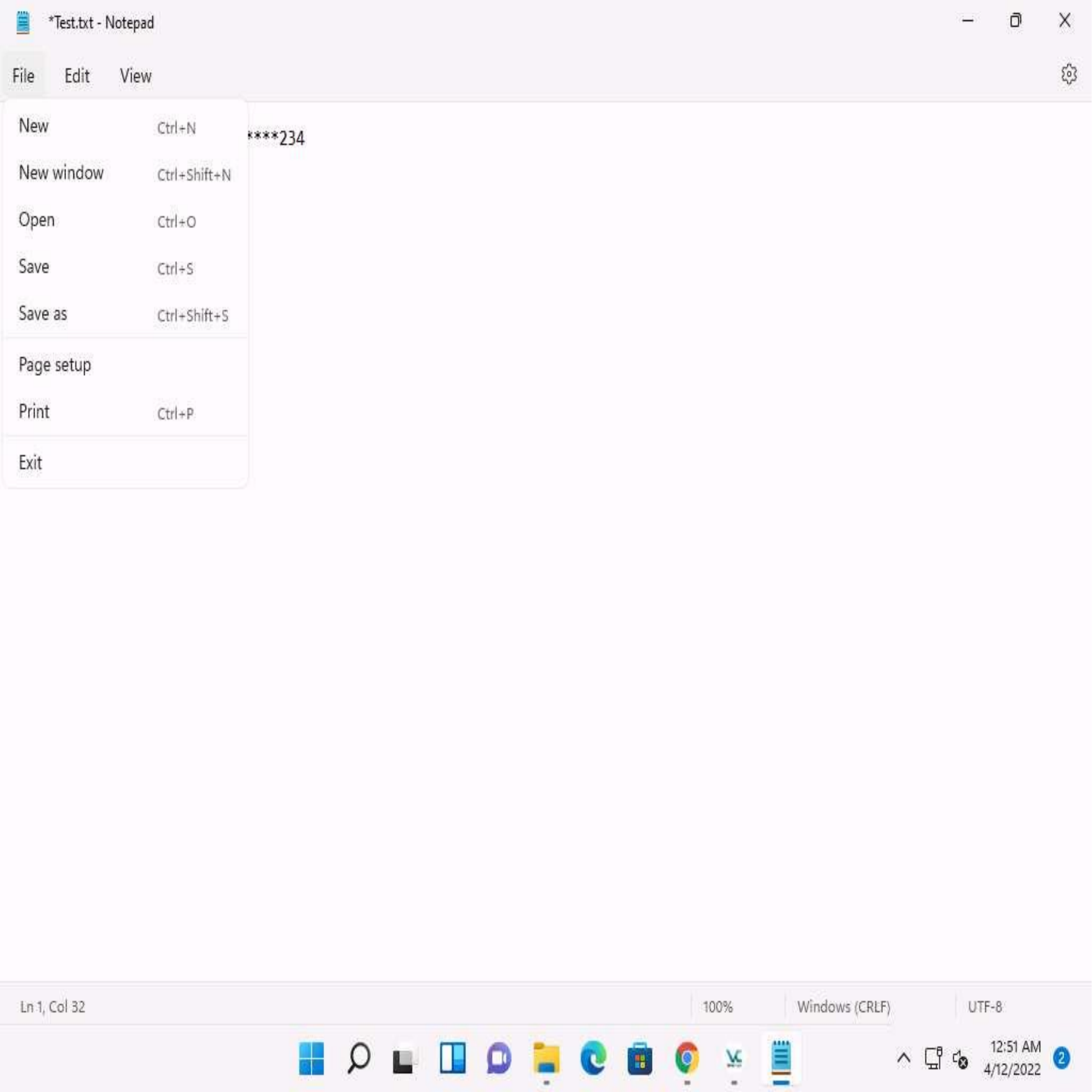
Volume: C:\Users\Admin\Desktop\MyVolume

☑ Never save history

24. ☐ **MyVolume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.

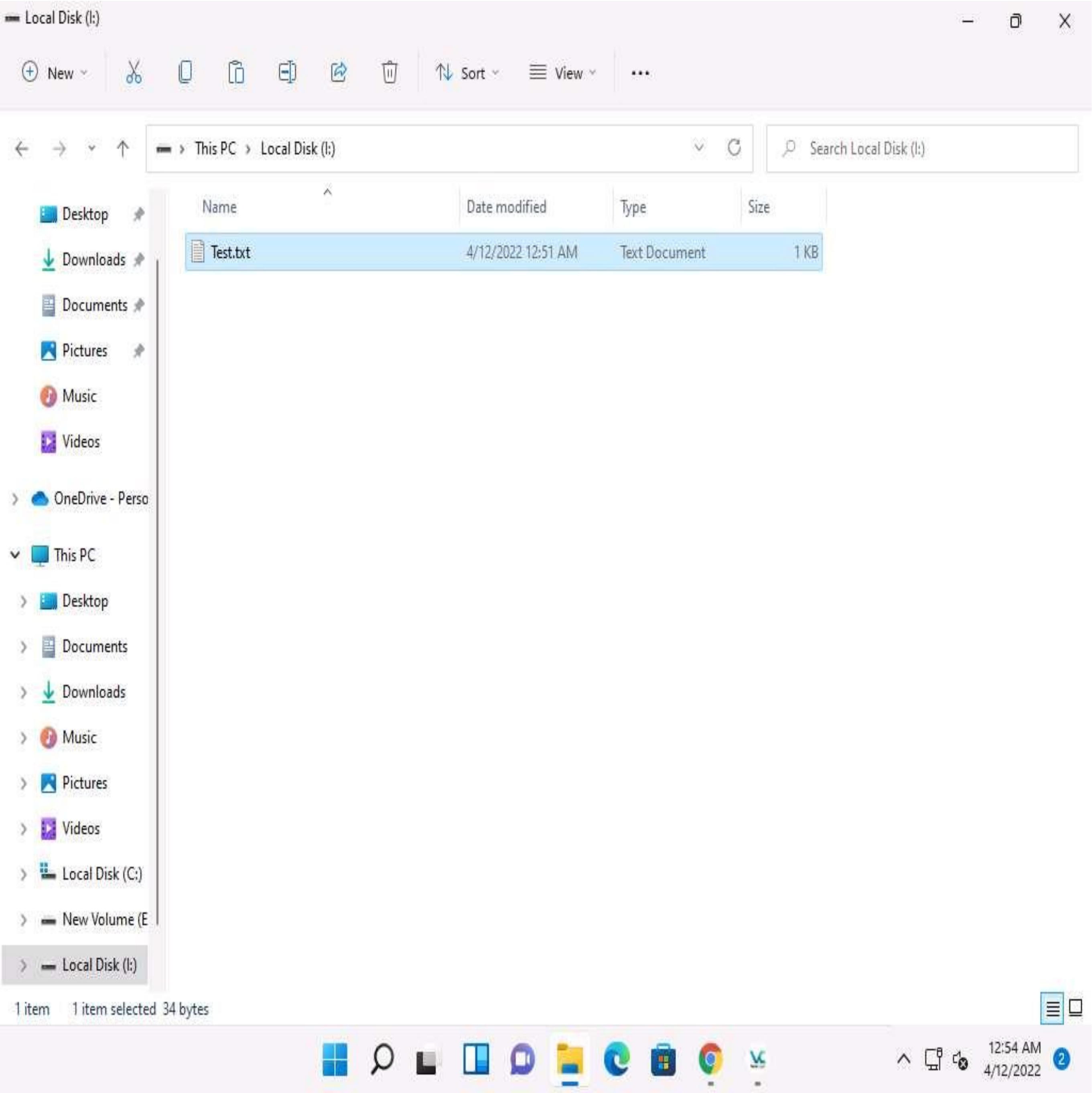
25. ☐ Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.

26. ☐ Click **File** in the menu bar and click **Save**.



****234

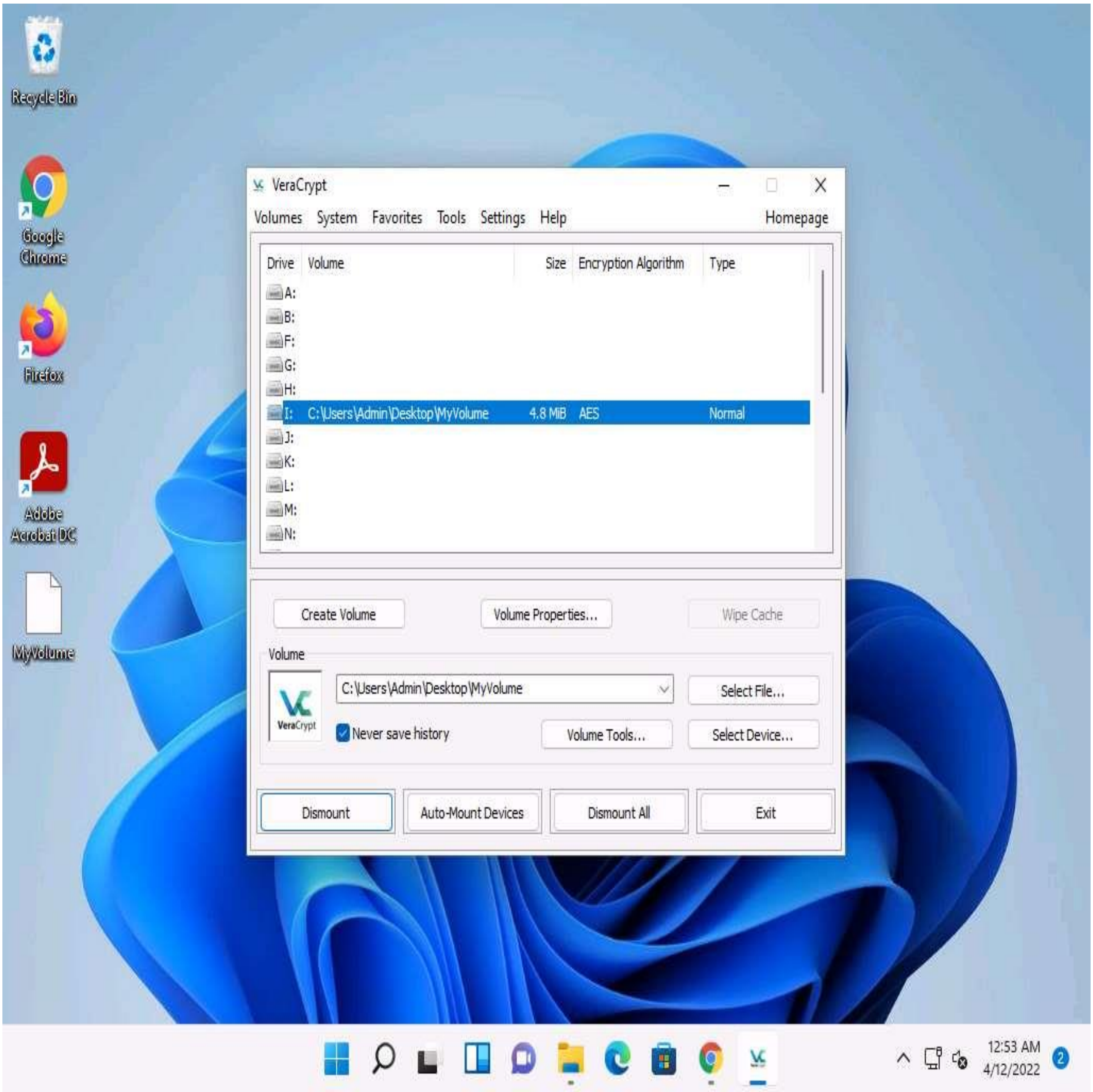
27. □ Copy the file from **Desktop** and paste it into **Local Disk** (**I:**). Close the window.



Name	Date modified	Type	Size
Test.txt	4/12/2022 12:51 AM	Text Document	1 KB

1 item 1 item selected 34 bytes

28. □ Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.



Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
F:				
G:				
H:				
I:	C:\Users\Admin\Desktop\MyVolume	4.8 MiB	AES	Normal
J:				
K:				
L:				
M:				
N:				

Volume: C:\Users\Admin\Desktop\MyVolume

☑ Never save history

29. □ The **I:** drive located in **This PC** disappears.

This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume—including its files—unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

30. □ This concludes the demonstration of performing disk encryption using VeraCrypt.

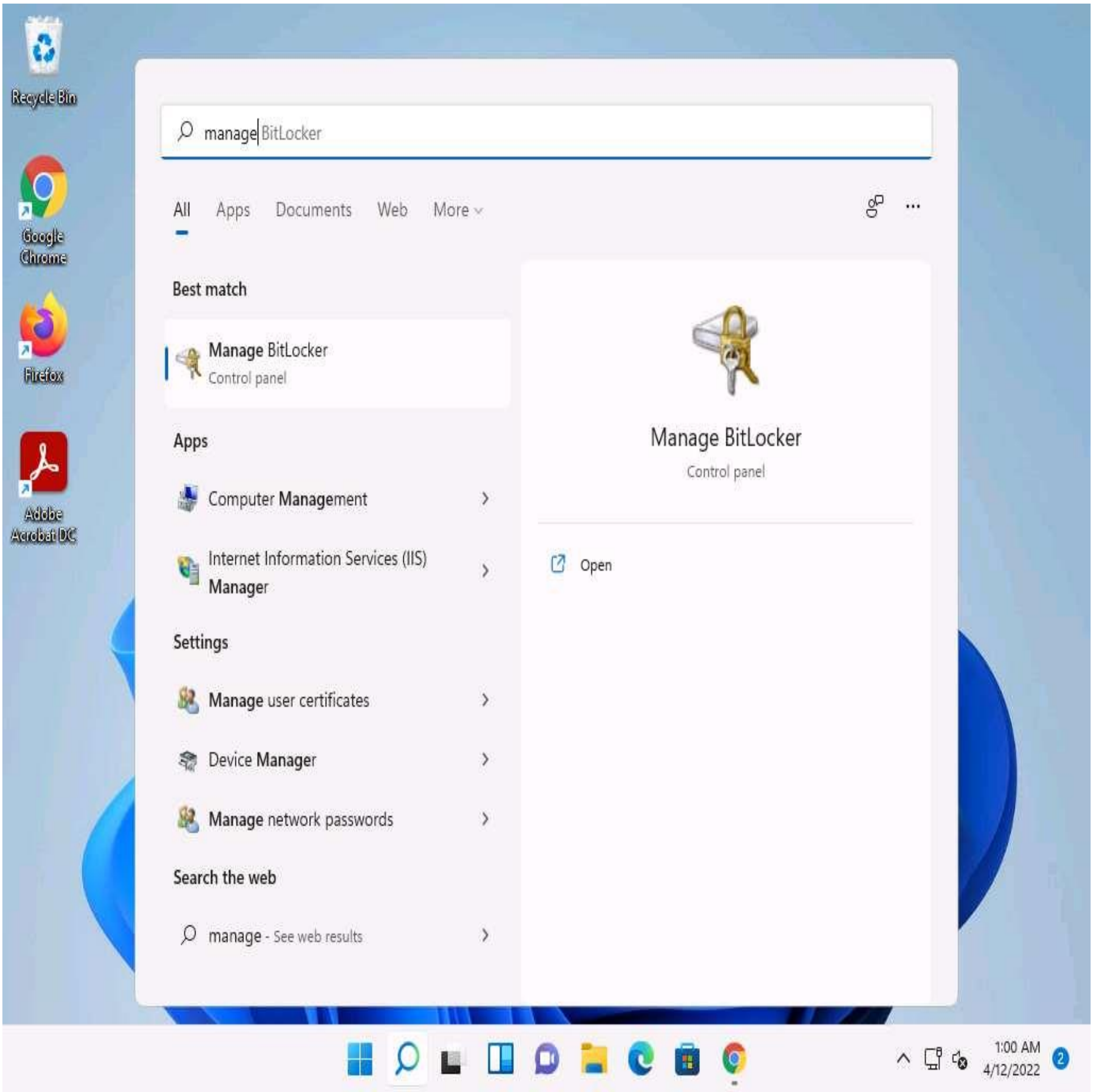
31. □ Close all open windows and document all the acquired information.

Task 2: Perform Disk Encryption using BitLocker Drive Encryption

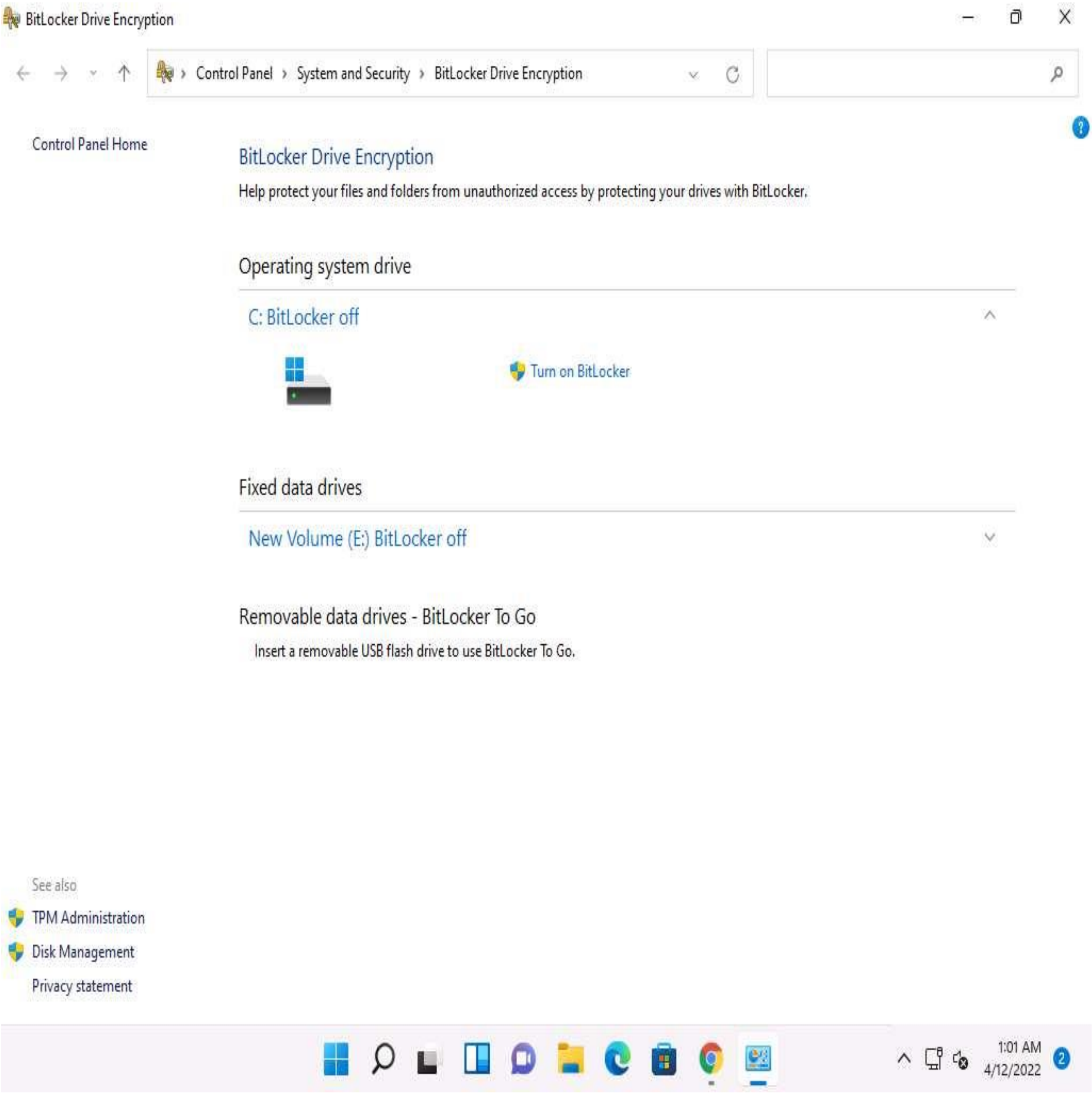
BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

Here, we will perform disk encryption using BitLocker Drive Encryption.

1. □ Click **Search** icon ( ) on the **Desktop**. Type **manage** in the search field, the **Manage Bitlocker** appears in the results, click **Open** to launch it.



2. □ The **BitLocker Drive Encryption** window appears; click the **New Volume (E:) BitLocker off** option under the **Fixed data drives** section.



BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

New Volume (E:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

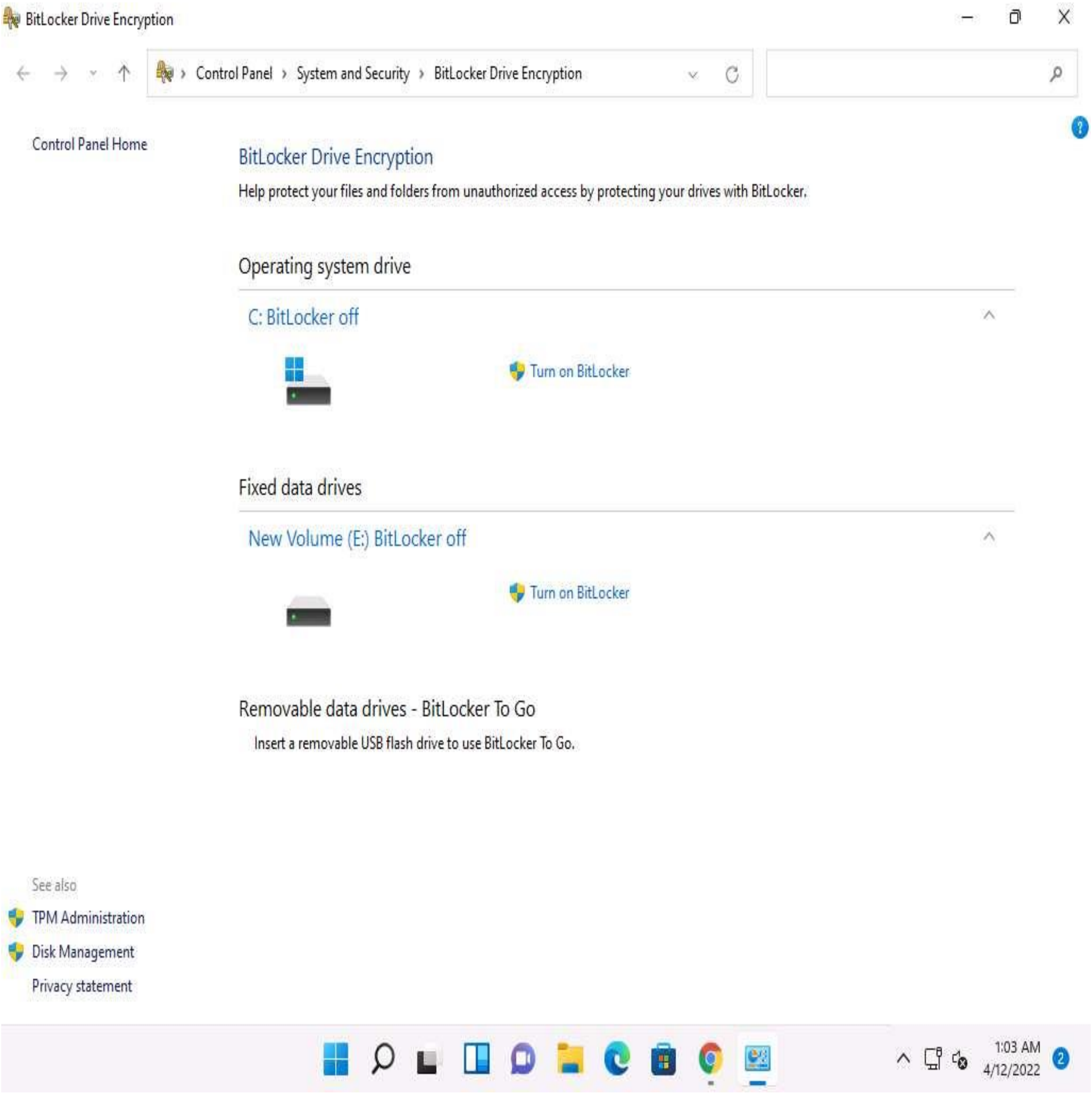
TPM Administration

Disk Management

Privacy statement

1:01 AM
4/12/2022

3. □ Click the **Turn on BitLocker** option under **New Volume (E:) BitLocker off**.


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

New Volume (E:) BitLocker off

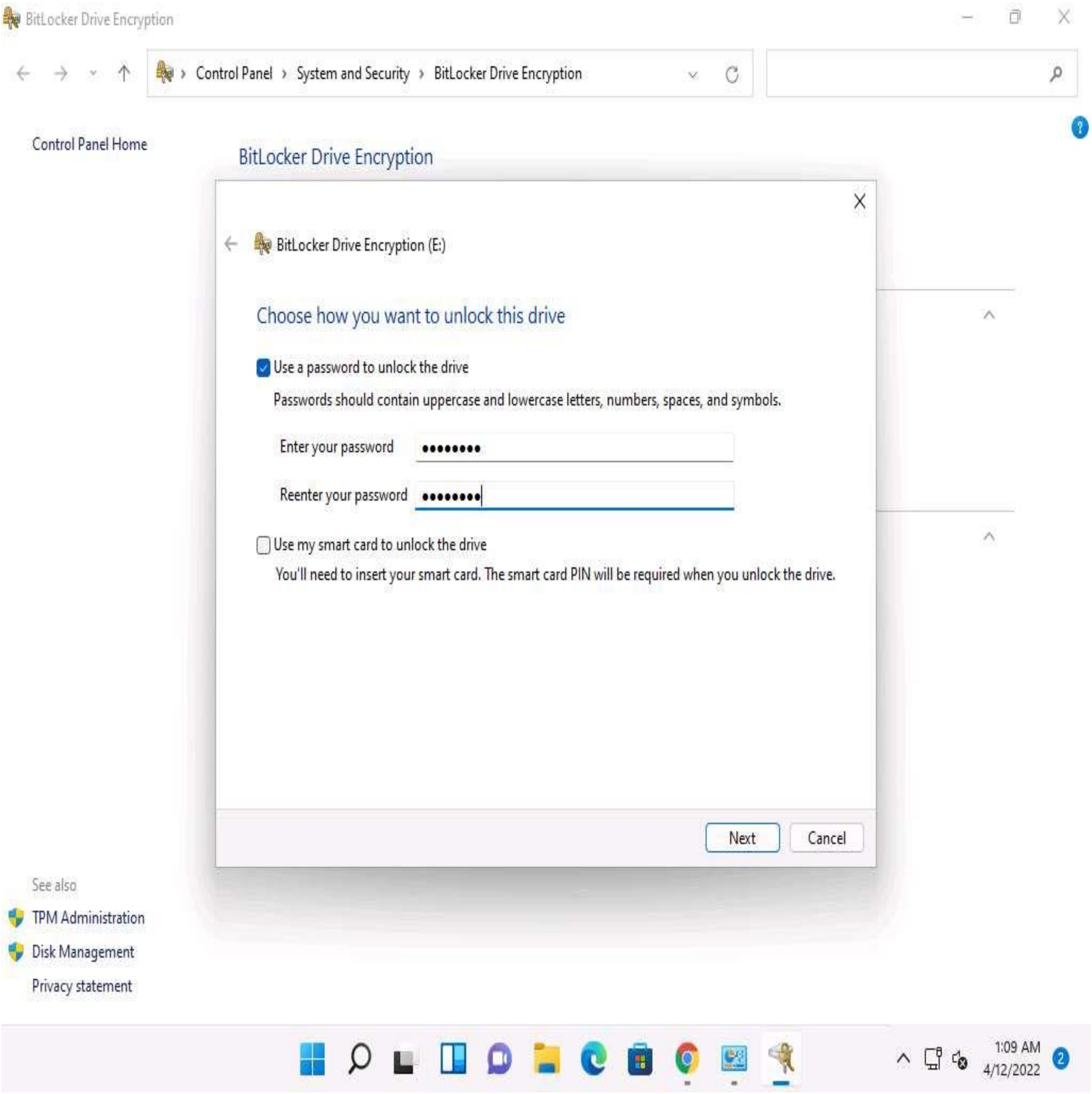
Turn on BitLocker

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

4. □ The **BitLocker Drive Encryption (E:)** wizard appears; check the **Use a password to unlock the drive** checkbox.

5. □ Type the password in the **Enter your password** field and re-type the password in the **Reenter your password** field; then, click **Next** (Here, the password entered is **test@123**).



BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

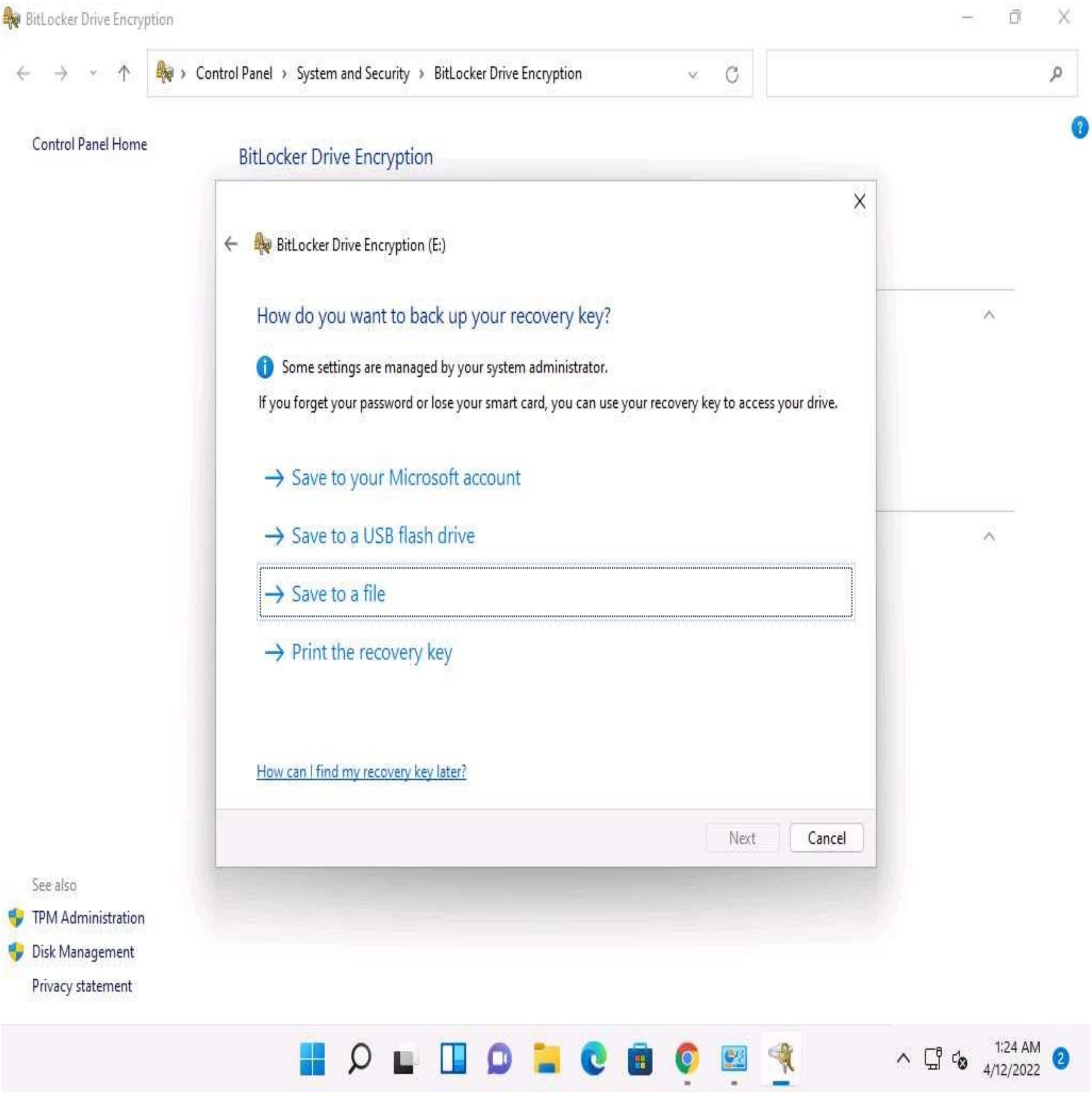
Enter your password ••••••••

Reenter your password ••••••••

☐ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

6. ☐ The **How do you want to back up your recovery key?** step appears; click **Save to a file** from the available options.



BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Control Panel Home
BitLocker Drive Encryption
BitLocker Drive Encryption (E:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

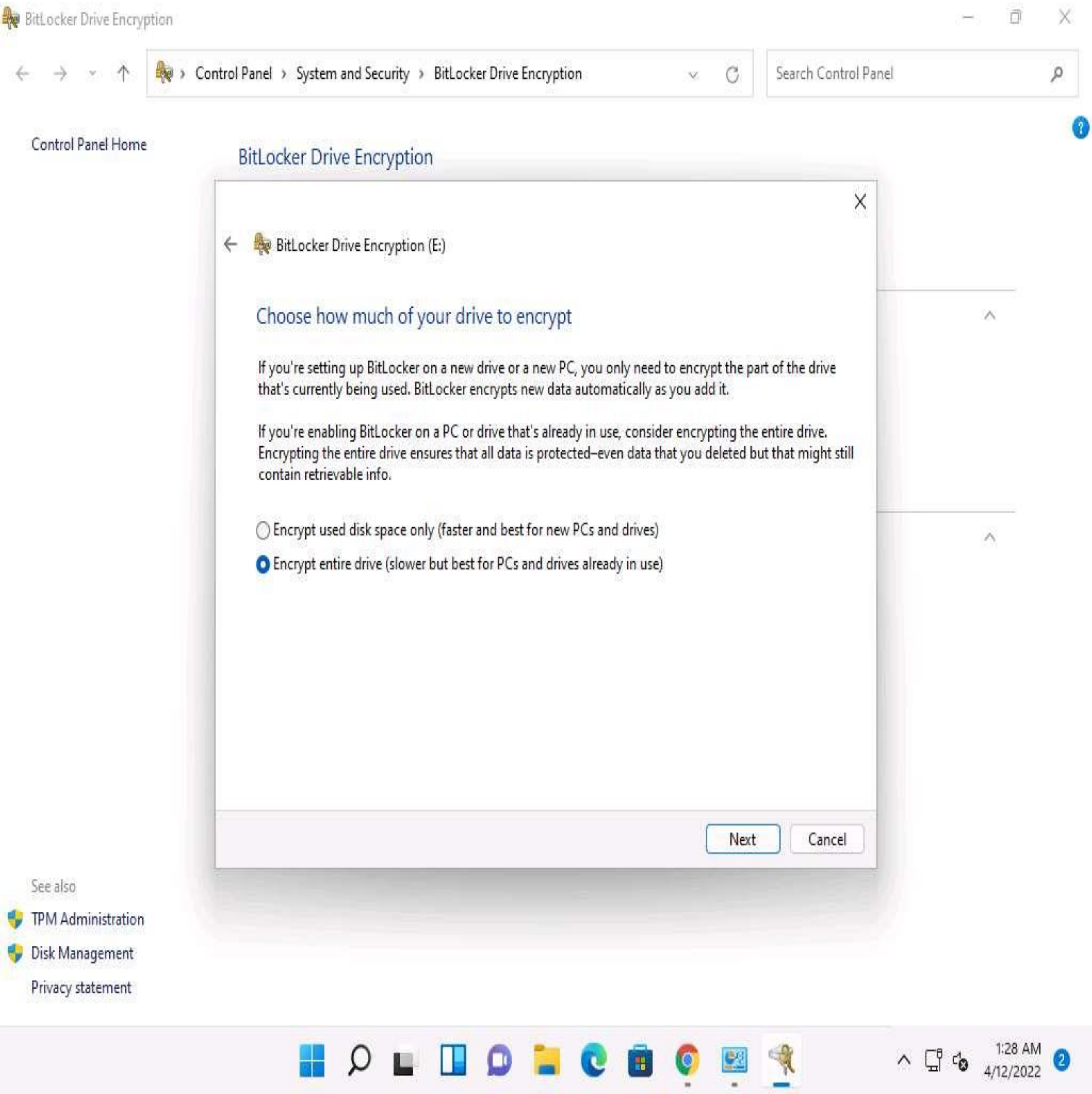
If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your Microsoft account
→ Save to a USB flash drive
→ Save to a file
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel
See also
TPM Administration
Disk Management
Privacy statement
1:24 AM
4/12/2022

7. □ The **Save BitLocker recovery key as** window appears; keep the save location set to **This PC --> Documents** and click **Save**.

8. □ Click **Next** in the **How do you want to back up your recovery key?** step.

9. □ In the **Choose how much of your drive to encrypt** step, select the **Encrypt entire drive (slower but best for PCs and drives already in use)** button, and click **Next**.



BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption
BitLocker Drive Encryption (E:)
See also
TPM Administration
Disk Management
Privacy statement
1:28 AM
4/12/2022

Choose how much of your drive to encrypt

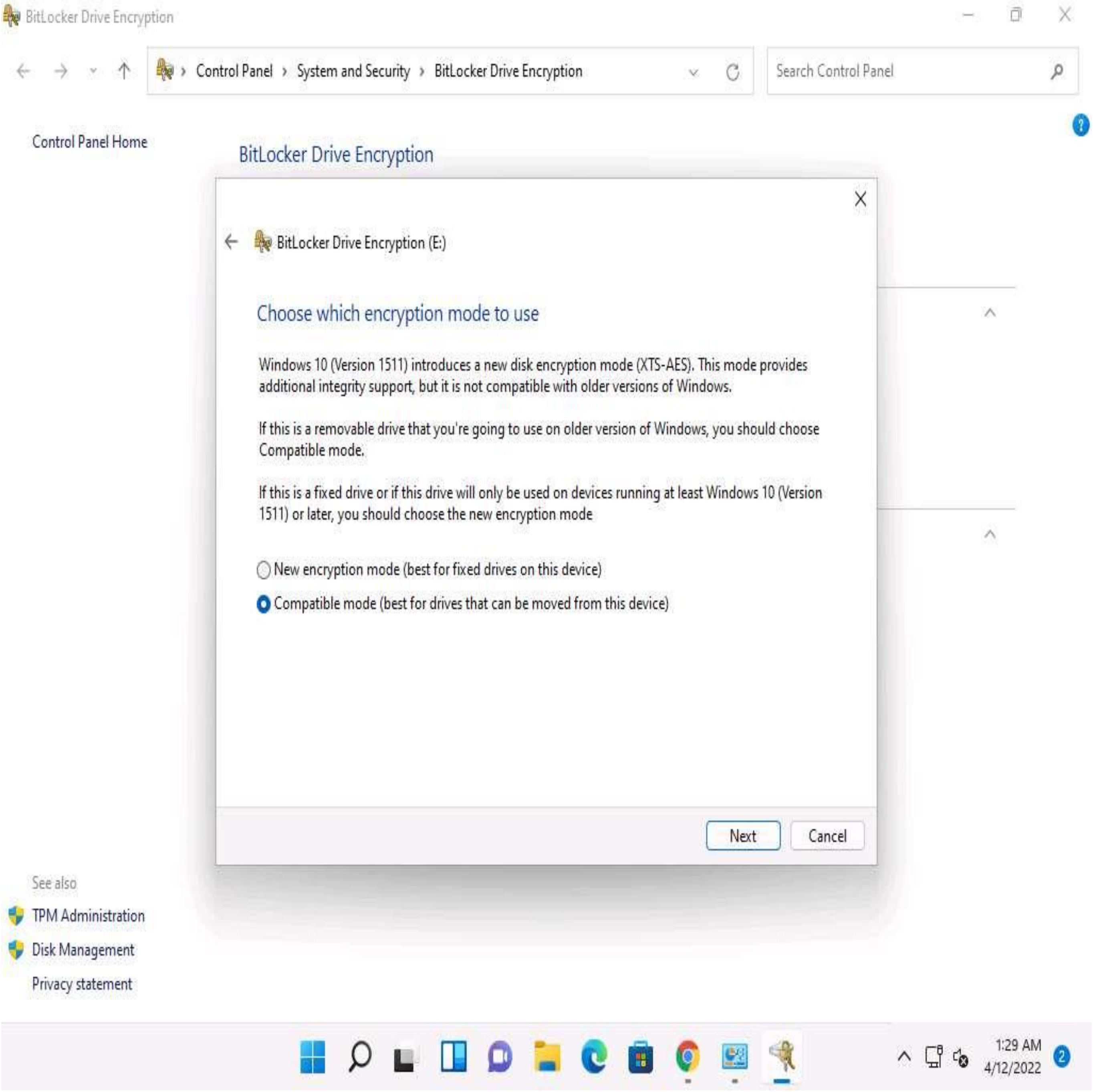
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

○ Encrypt used disk space only (faster and best for new PCs and drives)

● Encrypt entire drive (slower but best for PCs and drives already in use)

10. □ In the **Choose which encryption mode to use** step, ensure that the **Compatible mode (best for drives that can be moved from this device)** option is selected, and click **Next**.


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption
See also
TPM Administration
Disk Management
Privacy statement
1:29 AM
4/12/2022

BitLocker Drive Encryption (E:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

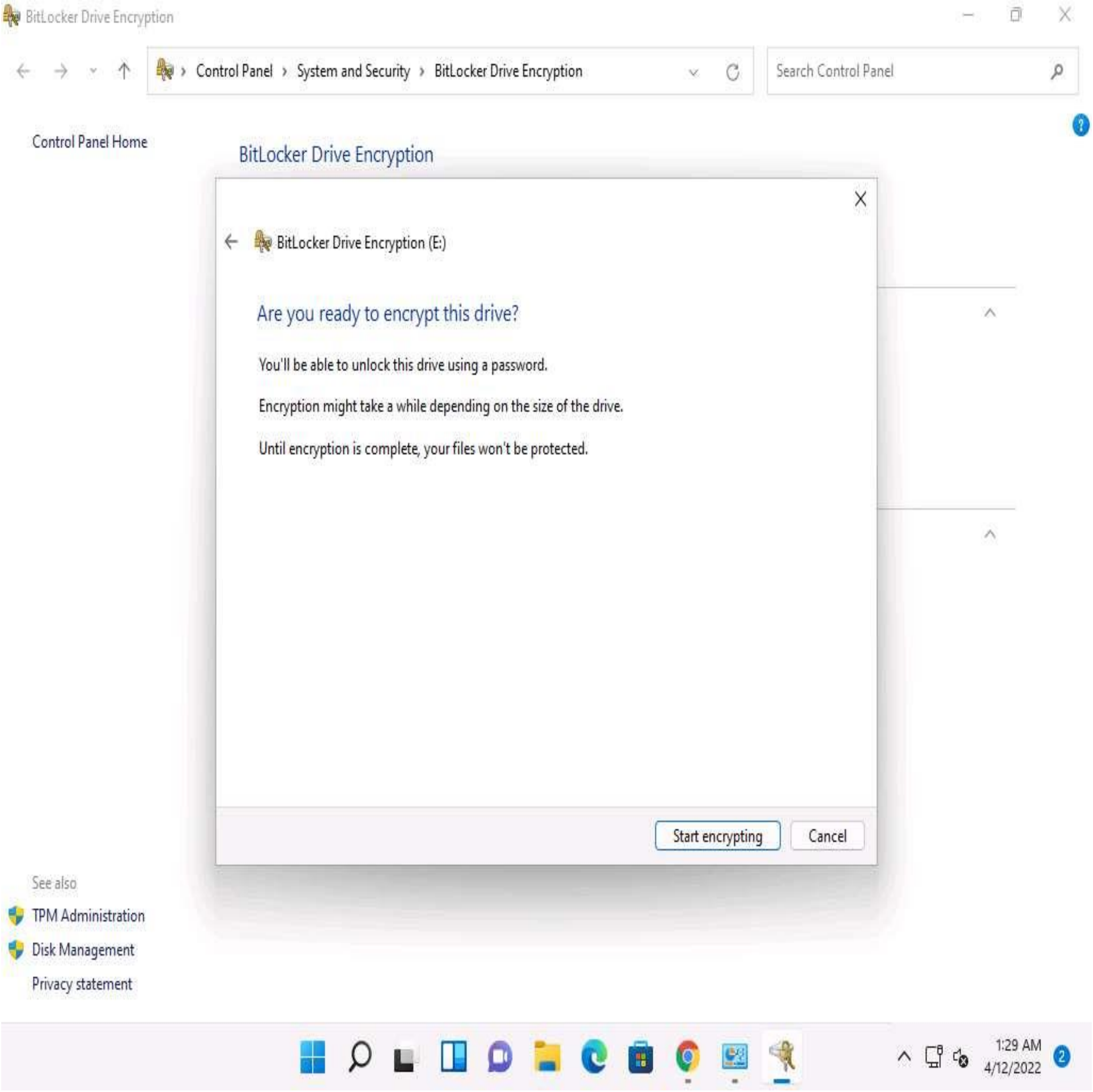
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)

● Compatible mode (best for drives that can be moved from this device)

11. □ In the **Are you ready to encrypt this drive?** step, click **Start encrypting** to encrypt the selected drive.



BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption
BitLocker Drive Encryption (E:)
Start encrypting
Cancel
See also
TPM Administration
Disk Management
Privacy statement
1:29 AM
4/12/2022

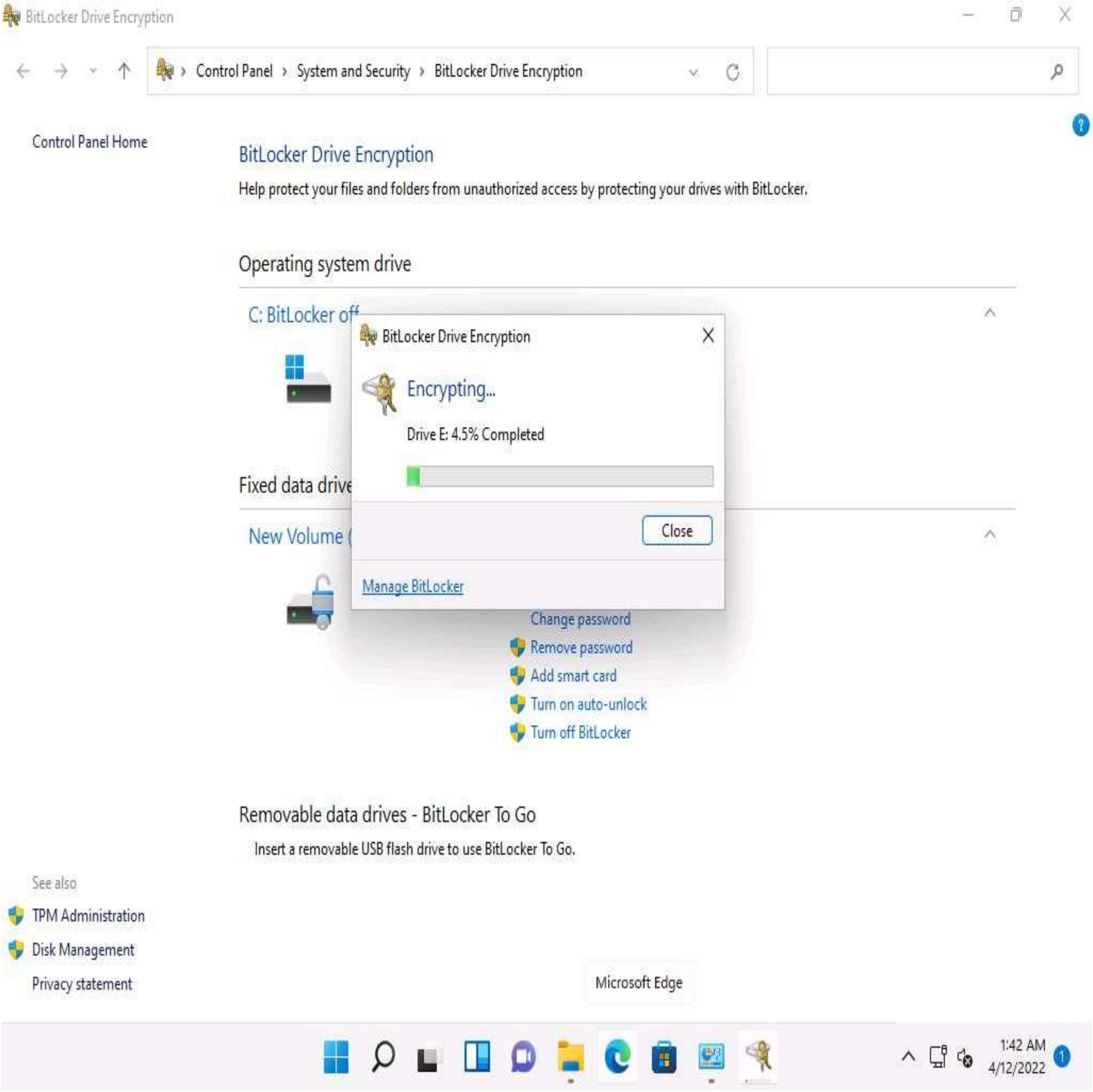
Are you ready to encrypt this drive?

You'll be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

12. □ The **BitLocker Drive Encryption** pop-up appears, showing the **Encrypting...** status.



BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Fixed data drive

New Volume (

Change password

Remove password

Add smart card

Turn on auto-unlock

Turn off BitLocker

BitLocker Drive Encryption

Encrypting...

Drive E: 4.5% Completed

Close

Manage BitLocker

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

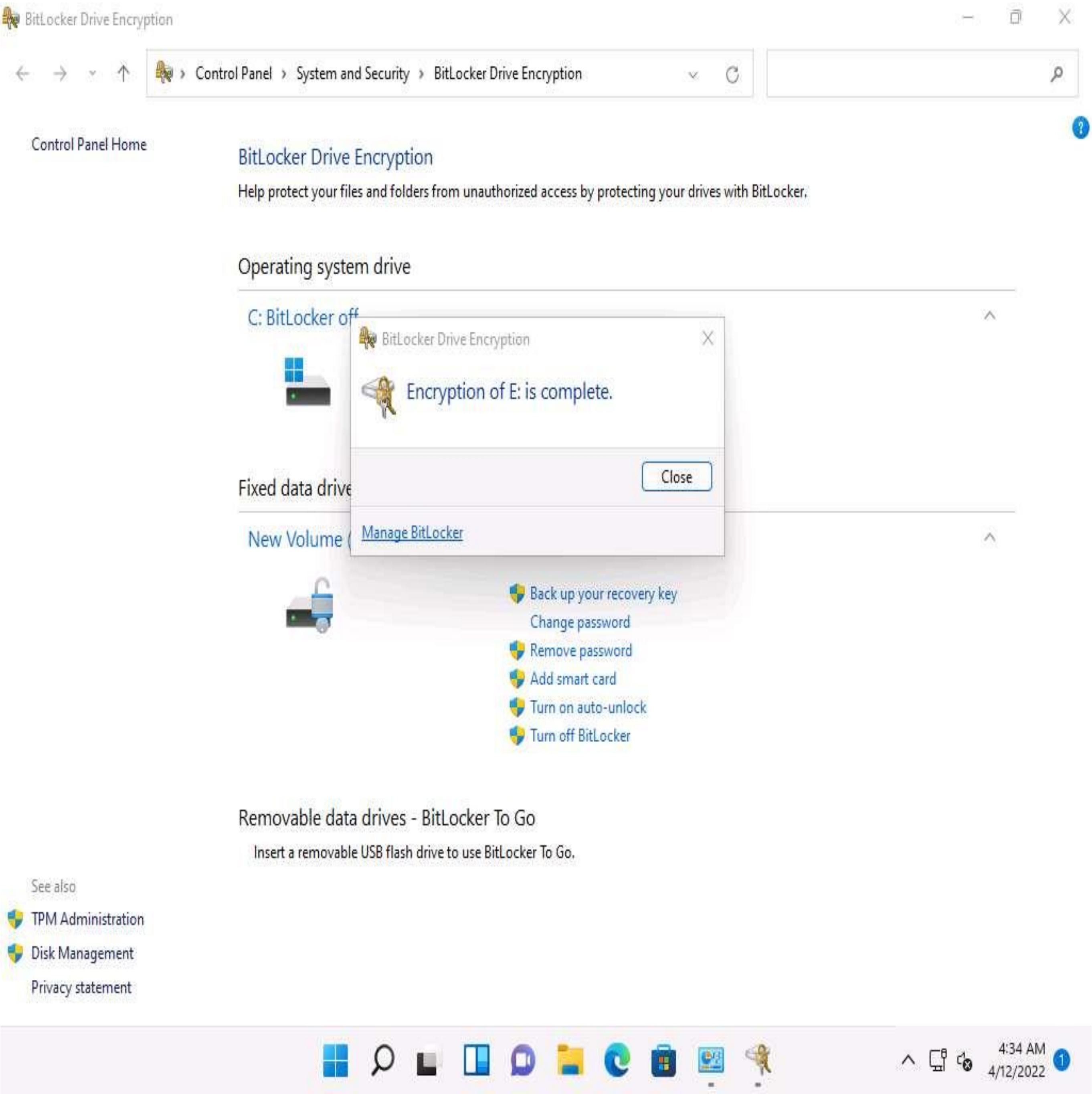
See also

TPM Administration

Disk Management

Privacy statement

13. □ After the completion of the encryption process, the **Encryption of E: is complete** notification appears; click **Close** and **Restart** the machine.



BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Fixed data drive

New Volume (

BitLocker Drive Encryption

Encryption of E: is complete.

Close

Manage BitLocker

Back up your recovery key
Change password
Remove password
Add smart card
Turn on auto-unlock
Turn off BitLocker

Removable data drives - BitLocker To Go

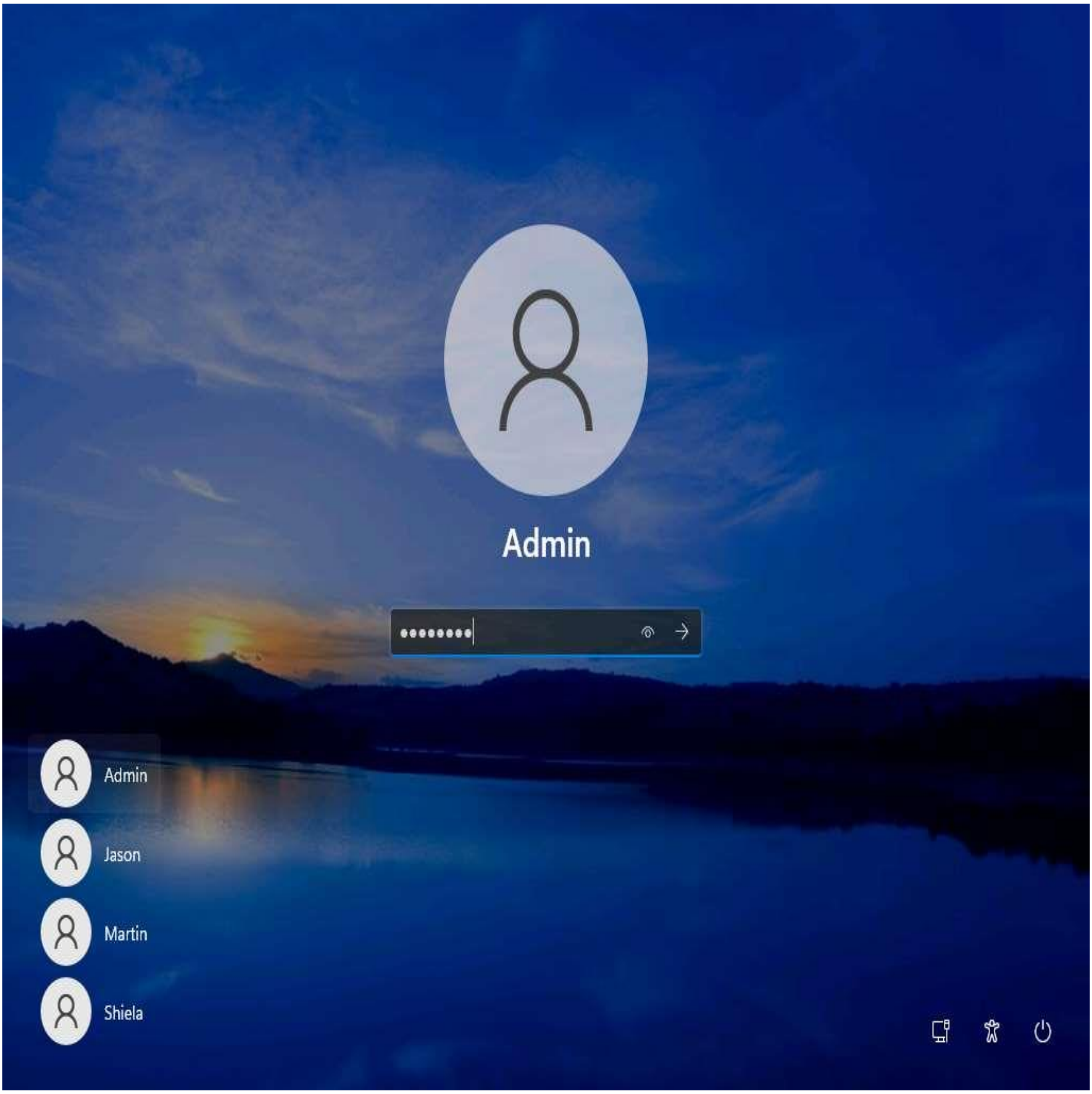
Insert a removable USB flash drive to use BitLocker To Go.

See also

TPM Administration
Disk Management
Privacy statement

4:34 AM
4/12/2022

14. □ After the system reboots, click Ctrl+Alt+Delete to activate it. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login

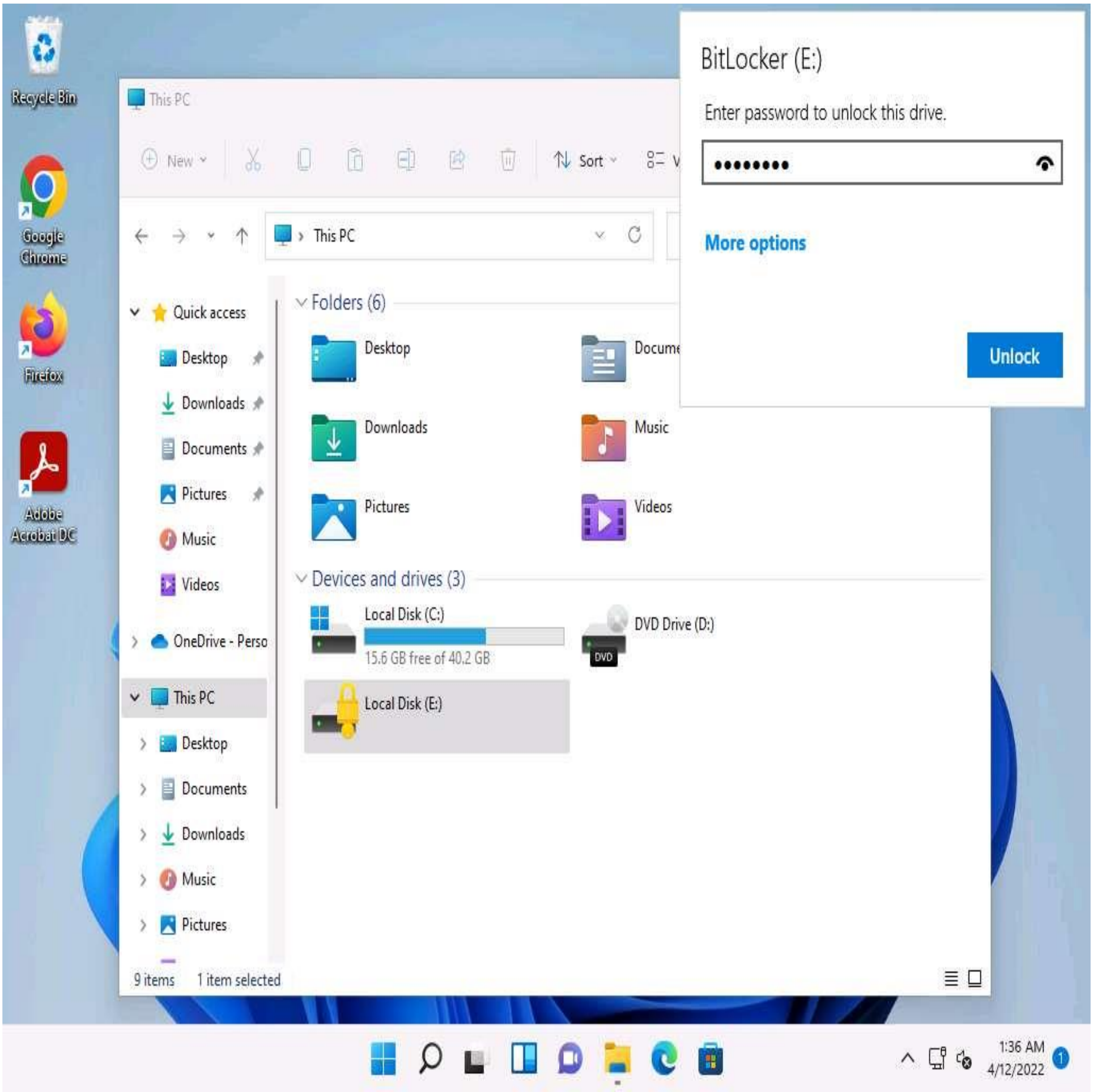


15. □ Open **File Explorer** and click **This PC** from the left pane.

16. □ You can observe that **Local Disk (E:)** is now encrypted; double-click and the **Local Disk (E:)** security pop-up appears at the top-right corner of **Desktop**

17. □ Type the password you provided in **Step#5** and click **Unlock**.

Here, the password is **test@123**.



BitLocker (E:)

Enter password to unlock this drive.

••••••••

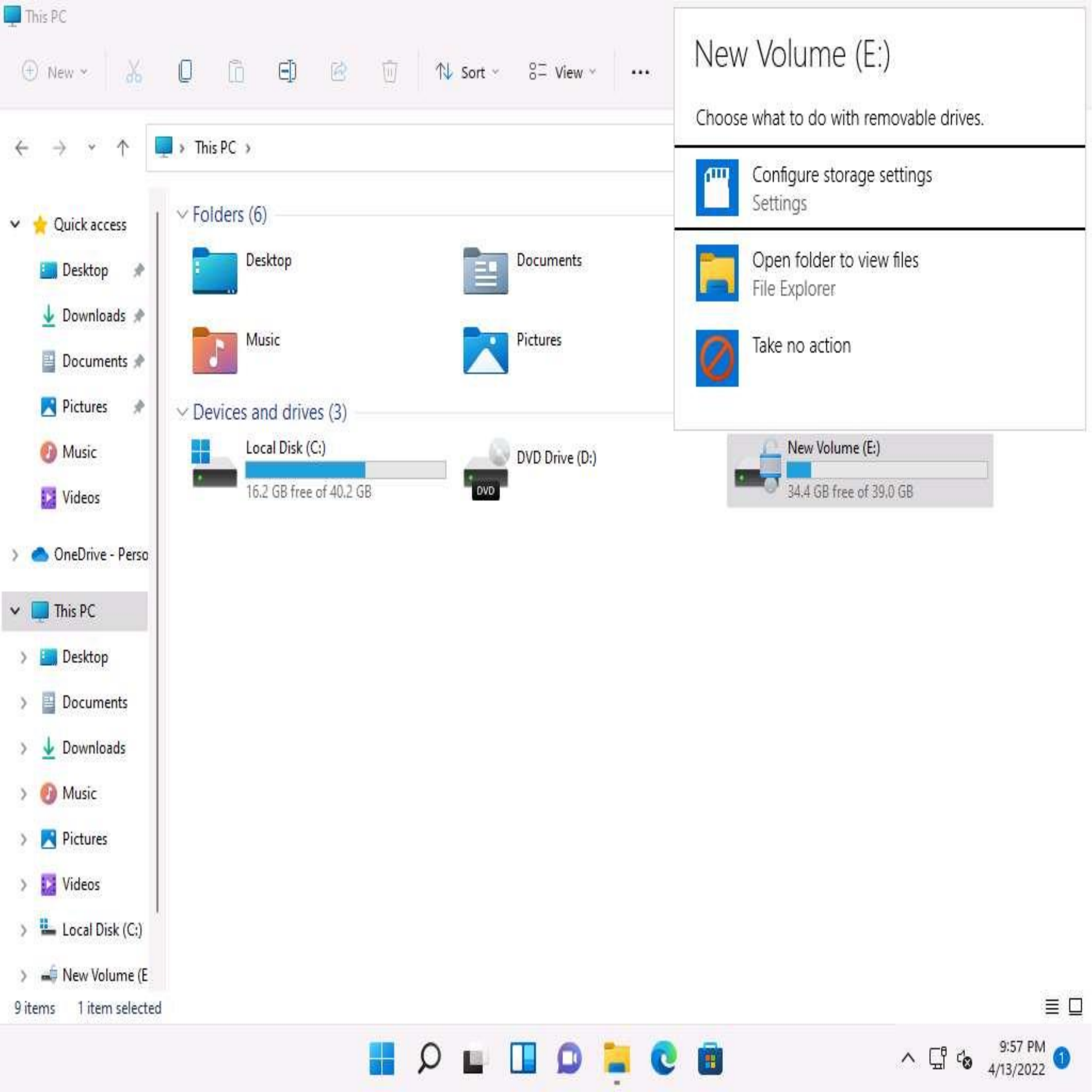
More options

Unlock

If the **Local Disk (E:)** pop-up appears at the top-right corner of the window. Click the **Open folder to view files** option to view the disk content.

18. ☐ The **New Volume (E:)** window appears displaying the disk content, as shown in the screenshot.

The disk will remain unlocked until the next time you restart the system.



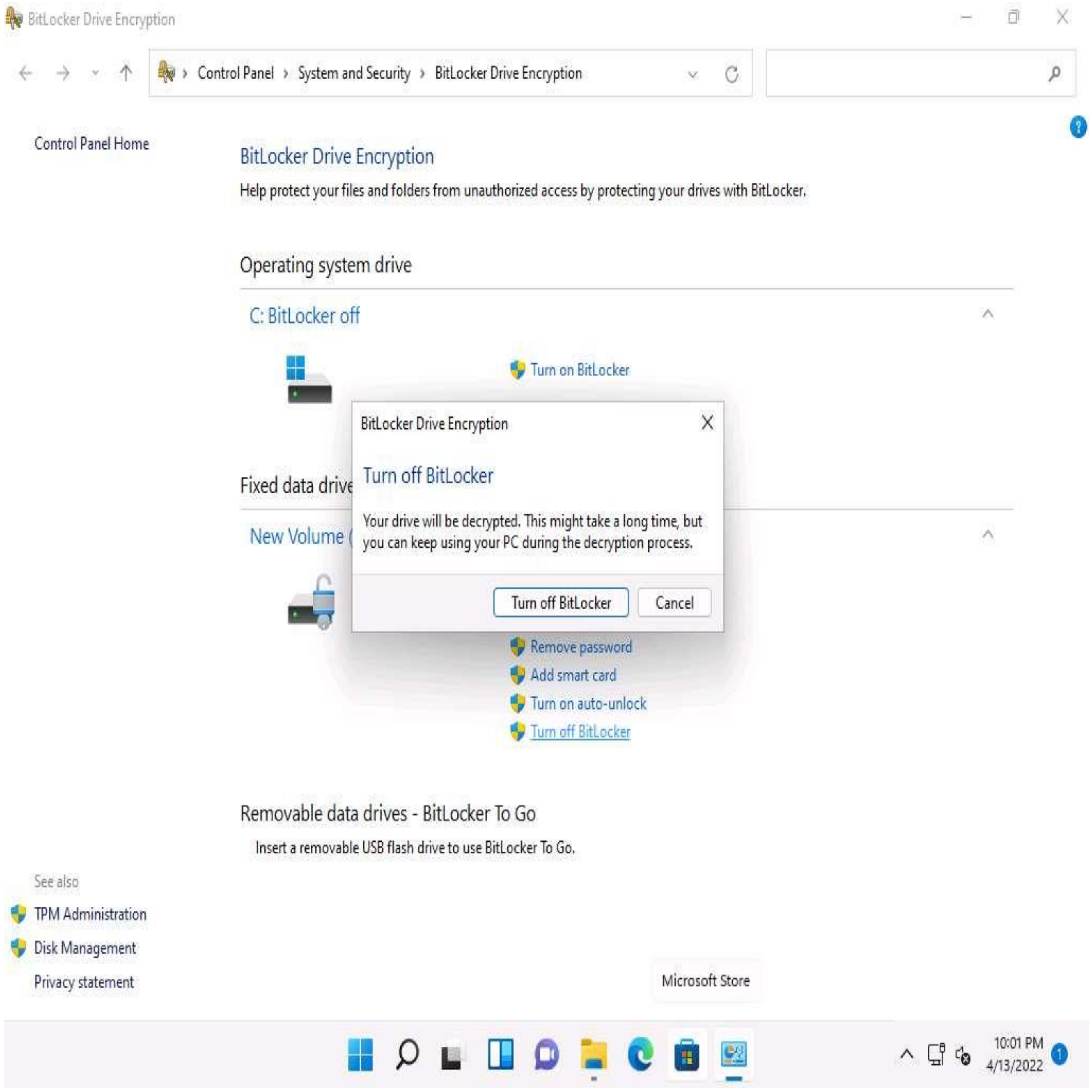
New Volume (E:)

Choose what to do with removable drives.

19. □ This concludes the demonstration of performing disk encryption using BitLocker Drive Encryption.

20. □ Once, you are done with this task; you must turn off BitLocker to decrypt the **New Volume (E:)** disk.

21. □ To do so, open the **BitLocker Drive Encryption** window, click **New Volume (E:) BitLocker on** and from the options click **Turn off BitLocker**.



BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drive

New Volume (

BitLocker Drive Encryption

Turn off BitLocker

Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

Turn off BitLocker | Cancel

Remove password

Add smart card

Turn on auto-unlock

Turn off BitLocker

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

TPM Administration

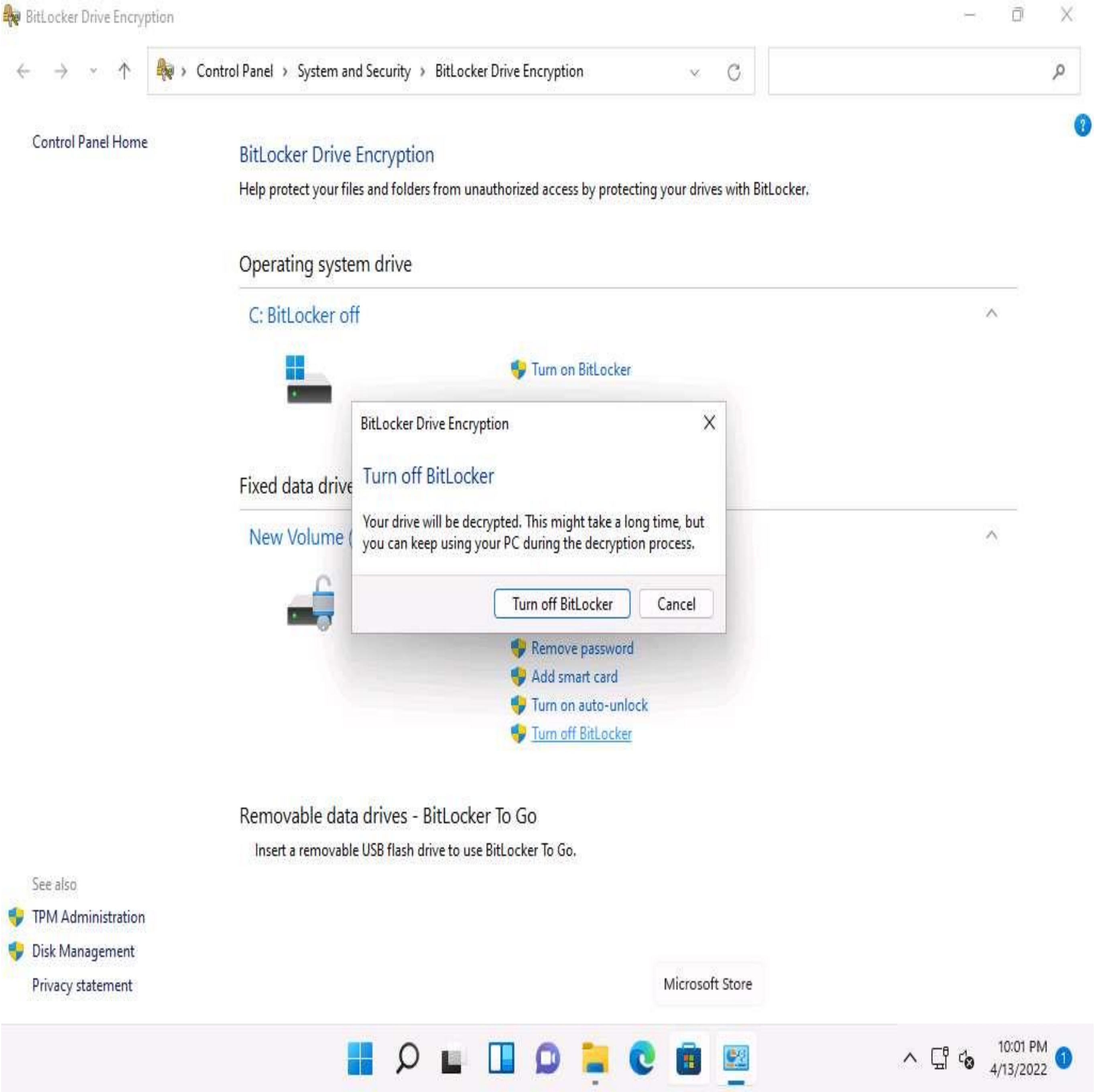
Disk Management

Privacy statement

Microsoft Store

10:01 PM
4/13/2022

22. □ The **BitLocker Drive Encryption** pop-up appears; click **Turn off BitLocker**.



BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

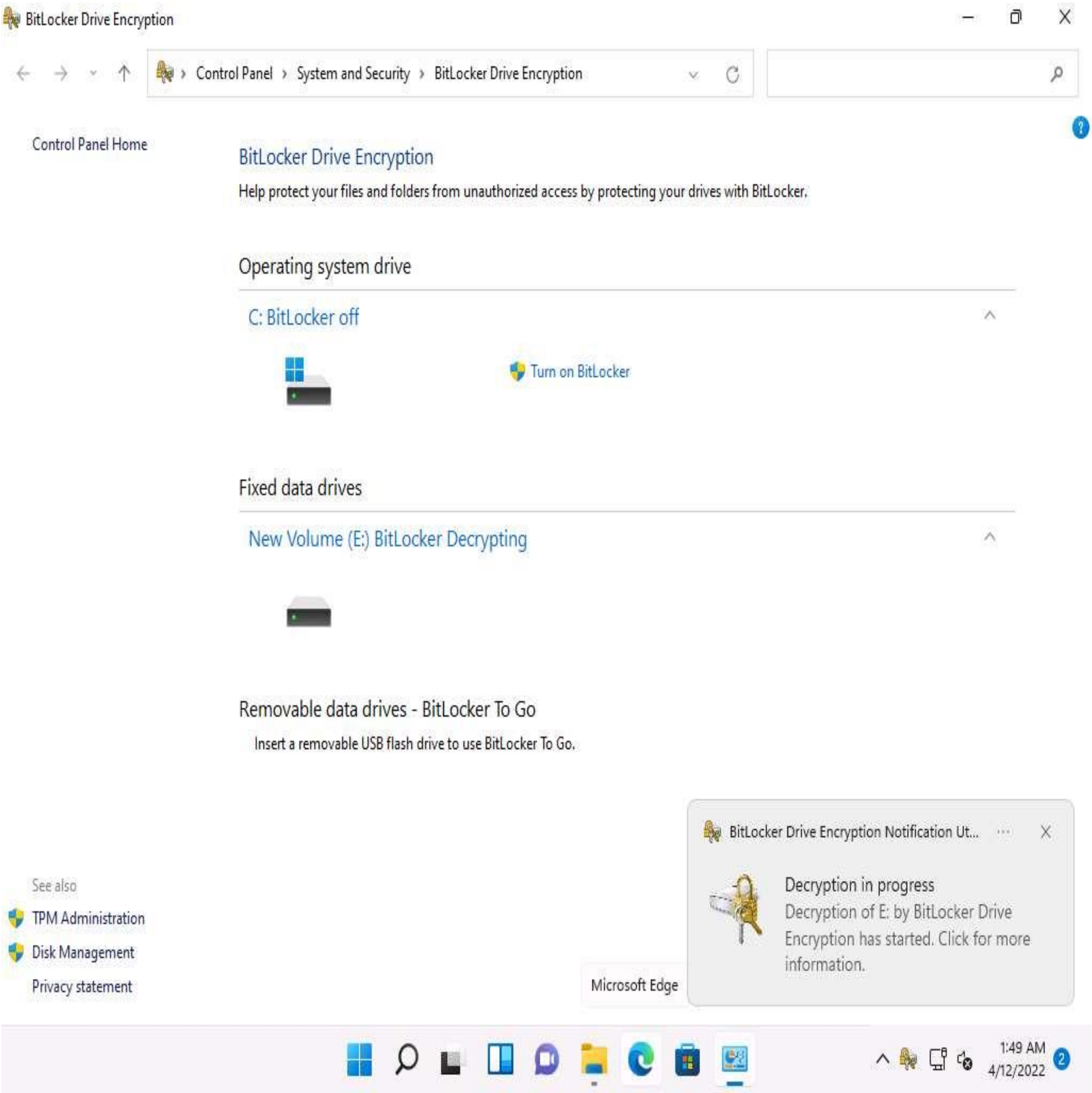
Turn off BitLocker

Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

23. □ **BitLocker** initiates the decryption process. Wait for it to complete.



BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Control Panel Home
BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.
Operating system drive
C: BitLocker off
Turn on BitLocker
Fixed data drives
New Volume (E:) BitLocker Decrypting
Removable data drives - BitLocker To Go
Insert a removable USB flash drive to use BitLocker To Go.
See also
TPM Administration
Disk Management
Privacy statement
Microsoft Edge
BitLocker Drive Encryption Notification Ut...
1:49 AM
4/12/2022

Decryption in progress
Decryption of E: by BitLocker Drive Encryption has started. Click for more information.

If after the completion of decryption process, the **Decryption of E: is complete** pop-up appears; click **Close**.

24. □ The **New Volume (E:)** decrypts successfully.
25. □ Close all open windows and document all the acquired information.

Task 3: Perform Disk Encryption using Rohos Disk Encryption

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly.

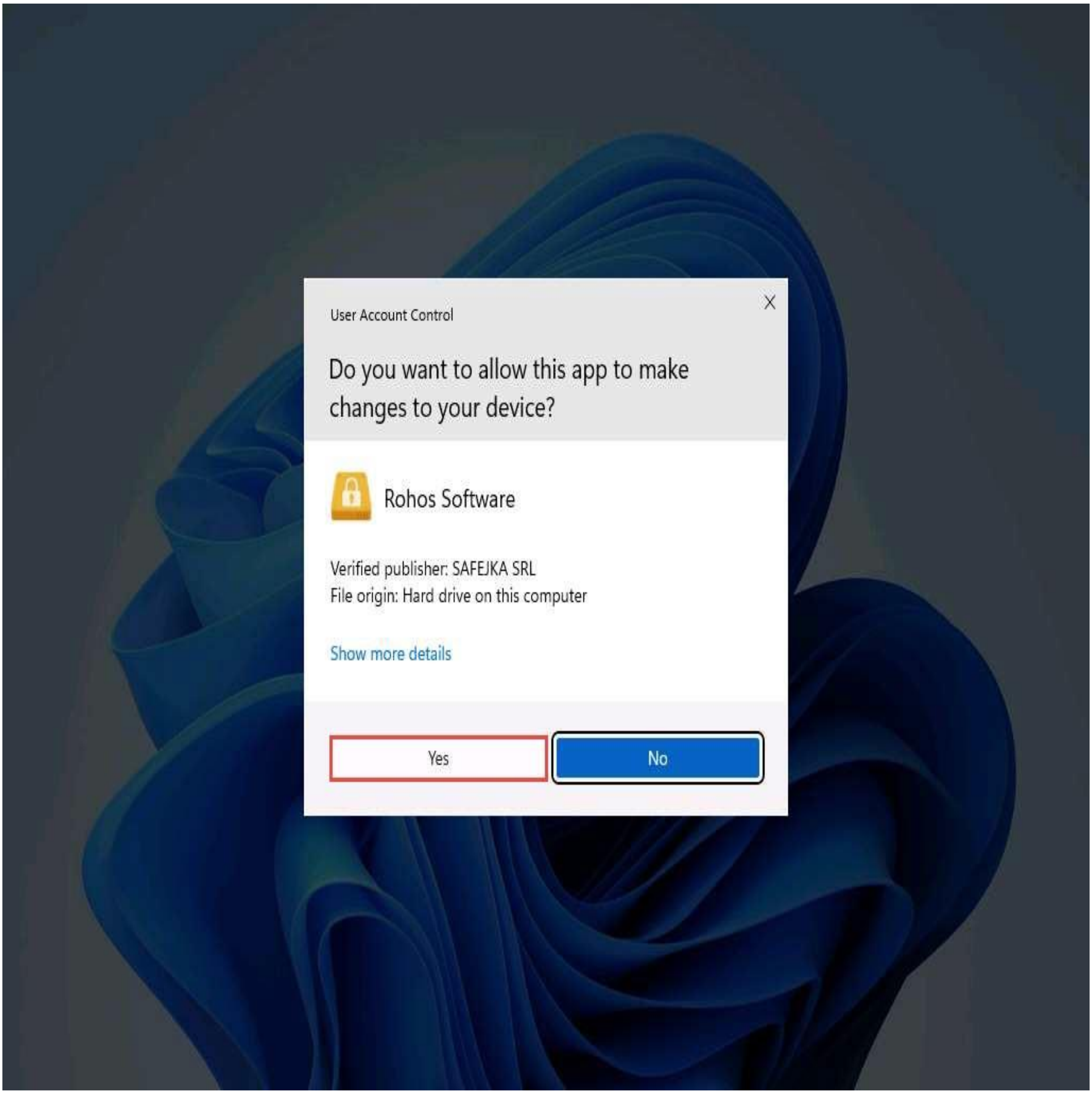
Here, we will use the Rohos Disk Encryption tool to perform disk encryption.

1. □ In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption** and double-click **rohos.exe**.

   If a **User Account Control** pop-up appears, click **Yes**.

2. □ The **Select Setup Language** dialog box appears; click **OK**.
3. □ The **Setup - Rohos Disk Encryption** window appears; read the instruction and click **Next**.
4. □ Follow the steps and install the application using all default settings.
5. □ After the completion of the installation, **Completing the Rohos Disk Encryption Setup** wizard appears; ensure that the **Launch Rohos Disk** checkbox is checked and click **Finish**.

   If **User Account Control** pop-up appears, click **Yes**.



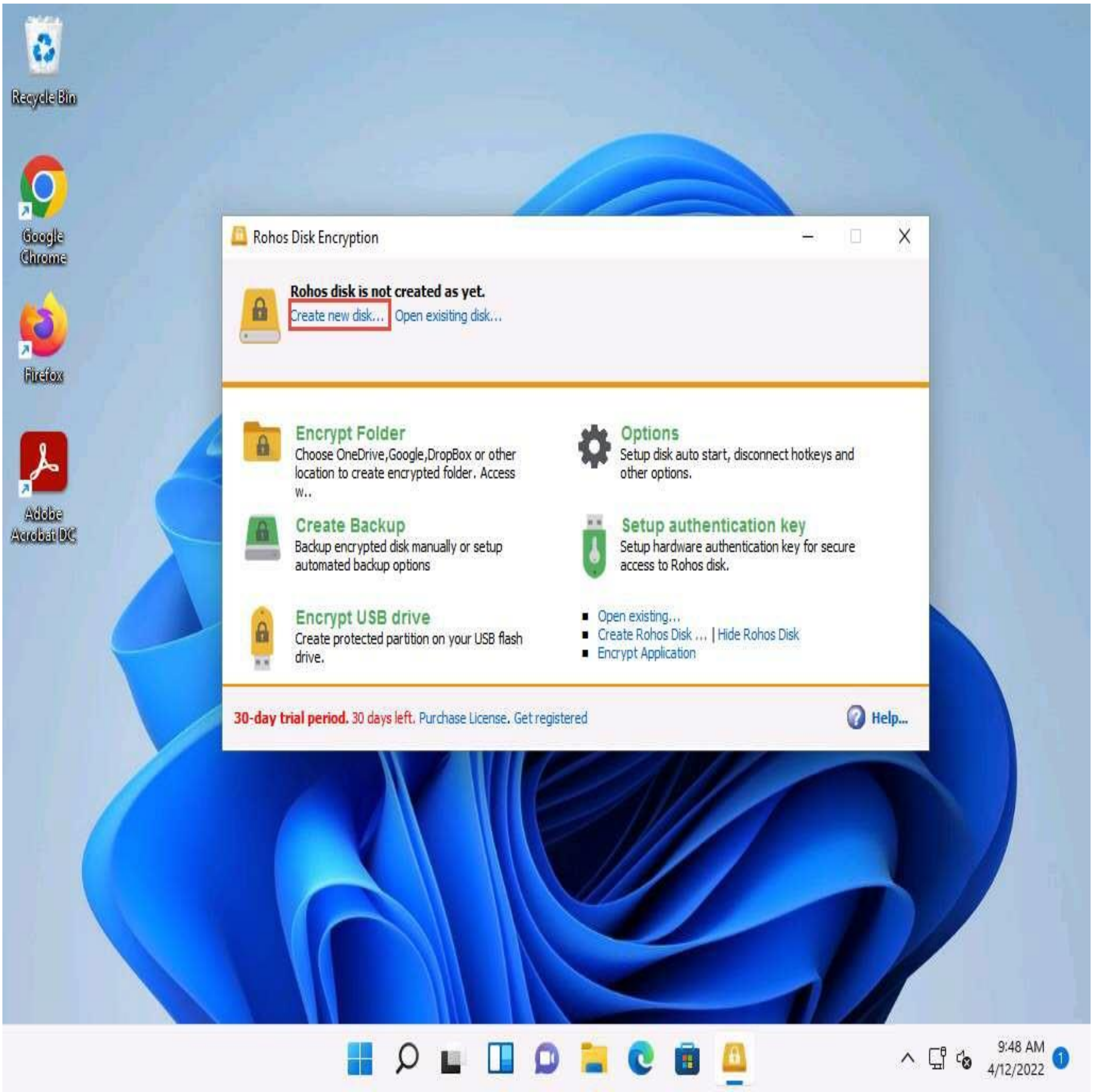
User Account Control

Do you want to allow this app to make changes to your device?

Rohos Software

Verified publisher: SAFEJKA SRL
File origin: Hard drive on this computer

6. □ The **Rohos Disk Encryption** main window appears; click **Create new disk...**



Rohos Disk Encryption

Rohos disk is not created as yet.
Create new disk... Open exisiting disk...

Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Options
Setup disk auto start, disconnect hotkeys and other options.

Create Backup
Backup encrypted disk manually or setup automated backup options

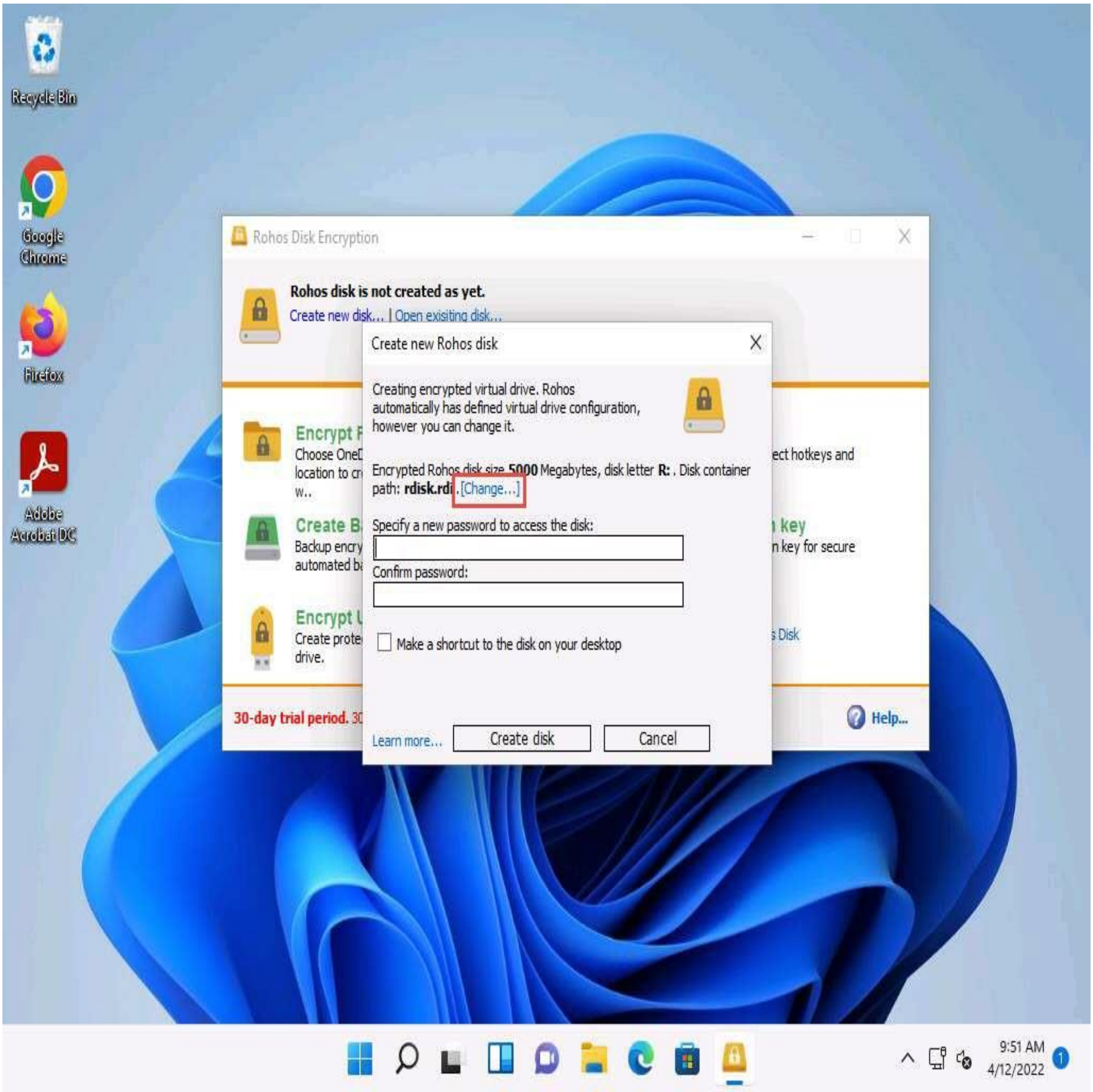
Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.

Encrypt USB drive
Create protected partition on your USB flash drive.

- Open existing...
- Create Rohos Disk ... | Hide Rohos Disk
- Encrypt Application

30-day trial period. 30 days left. Purchase License. Get registered   Help...

7. □ The **Create new Rohos disk** window appears; click **Change...** to modify the size of the encrypted disk.



Creating encrypted virtual drive. Rohos automatically has defined virtual drive configuration, however you can change it.

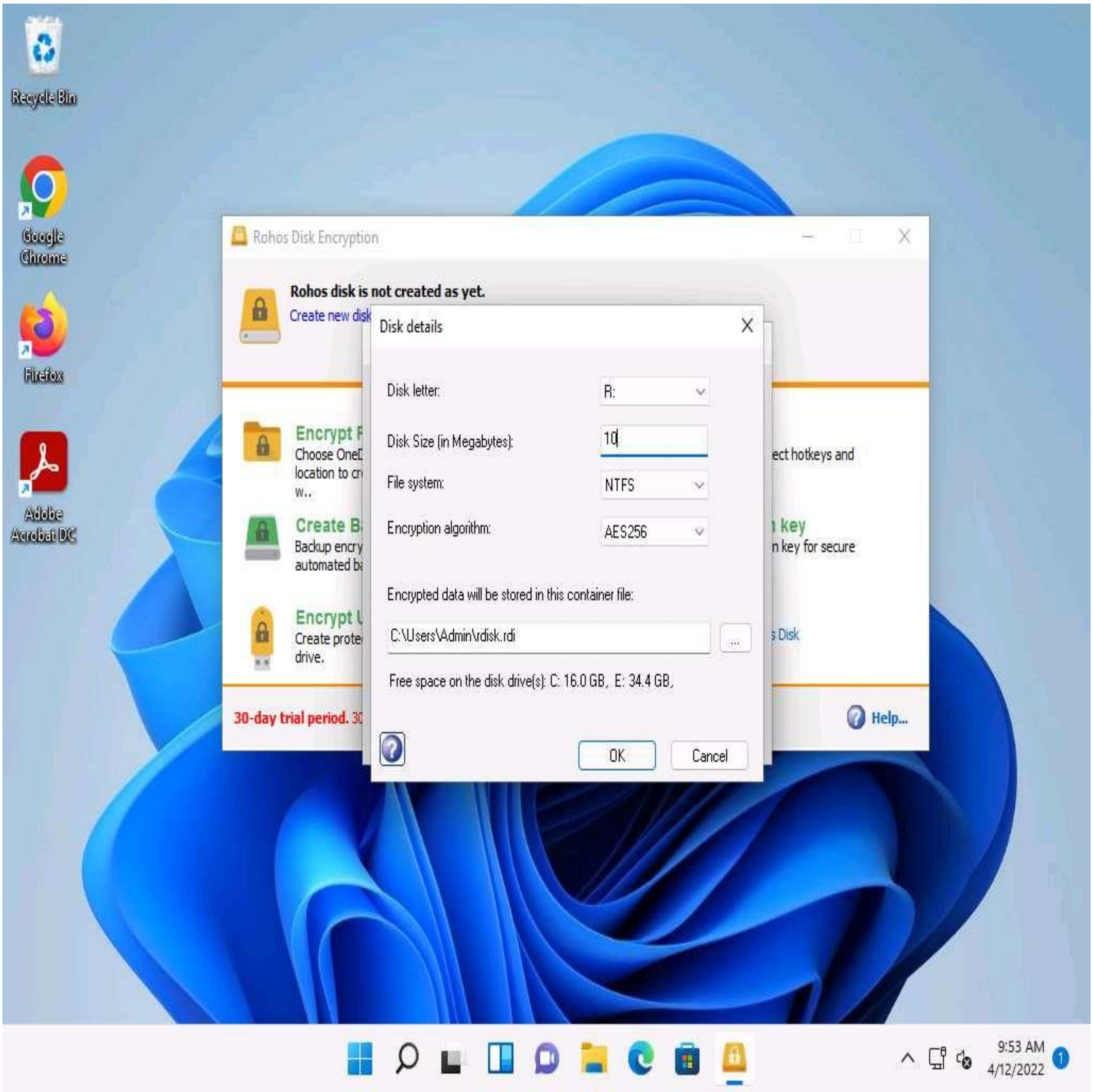
Encrypted Rohos disk size **5000** Megabytes, disk letter **R:** . Disk container path: **rdisk.rdi** .[Change...]

Specify a new password to access the disk:

Confirm password:

□ Make a shortcut to the disk on your desktop

8. □ The **Disk details** wizard appears; modify the disk size to **10** in the **Disk Size (in Megabytes)** field and leave all other settings to default; then, click **OK**.



Rohos disk is not created as yet.

Disk details

Disk letter: R:

Disk Size (in Megabytes): 10

File system: NTFS

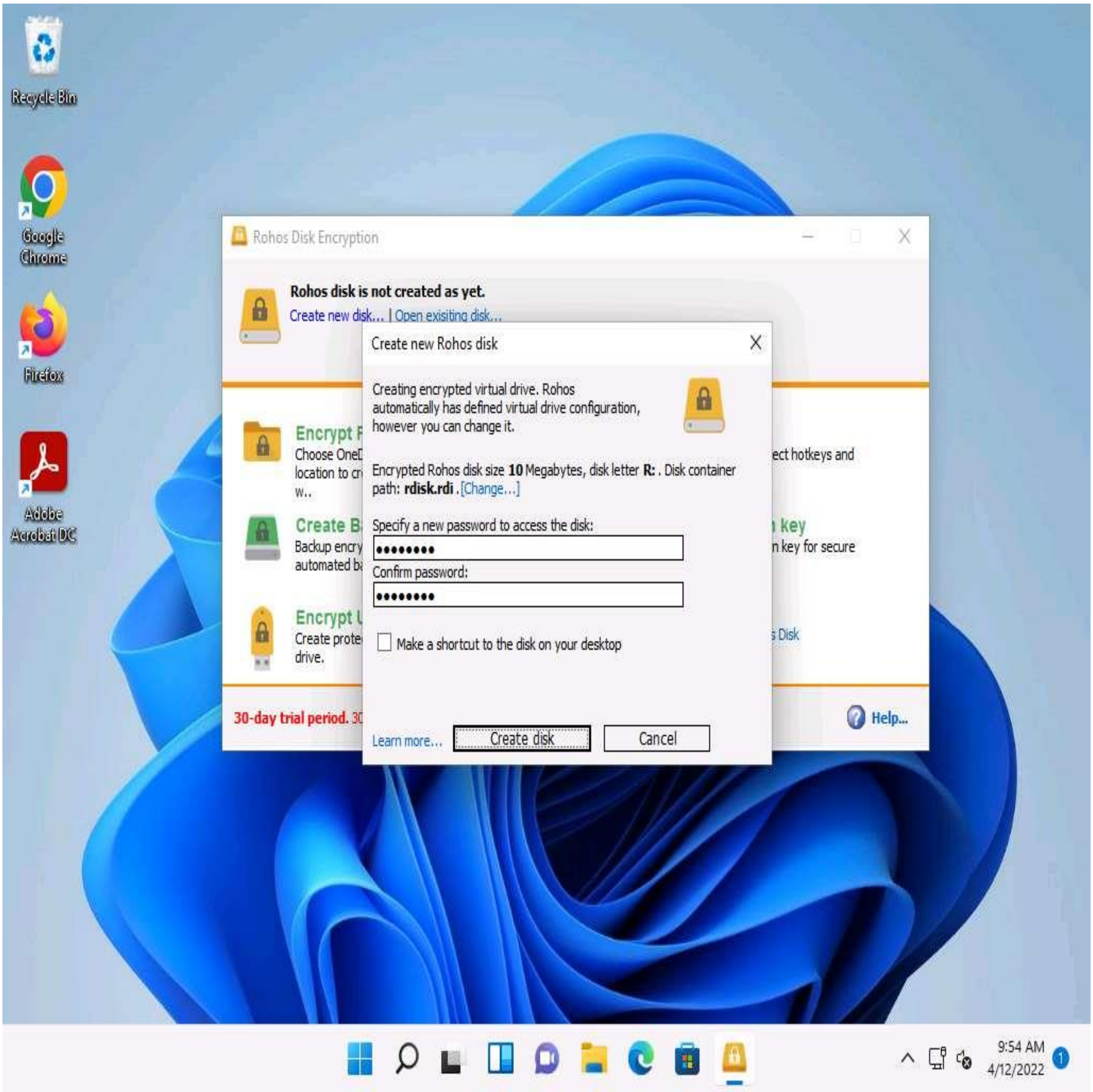
Encryption algorithm: AES256

Encrypted data will be stored in this container file:

C:\Users\Admin\rdisk.rdi

Free space on the disk drive(s): C: 16.0 GB, E: 34.4 GB,

9. □ Provide a password in the **Specify a new password to access the disk** field and retype it into the **Confirm password** field; then, click **Create disk** button (Here, the password provided is **test@123**).



Create new Rohos disk

Creating encrypted virtual drive. Rohos automatically has defined virtual drive configuration, however you can change it.

Encrypted Rohos disk size **10** Megabytes, disk letter **R:** . Disk container path: **rdisk.rdi** . [Change...]

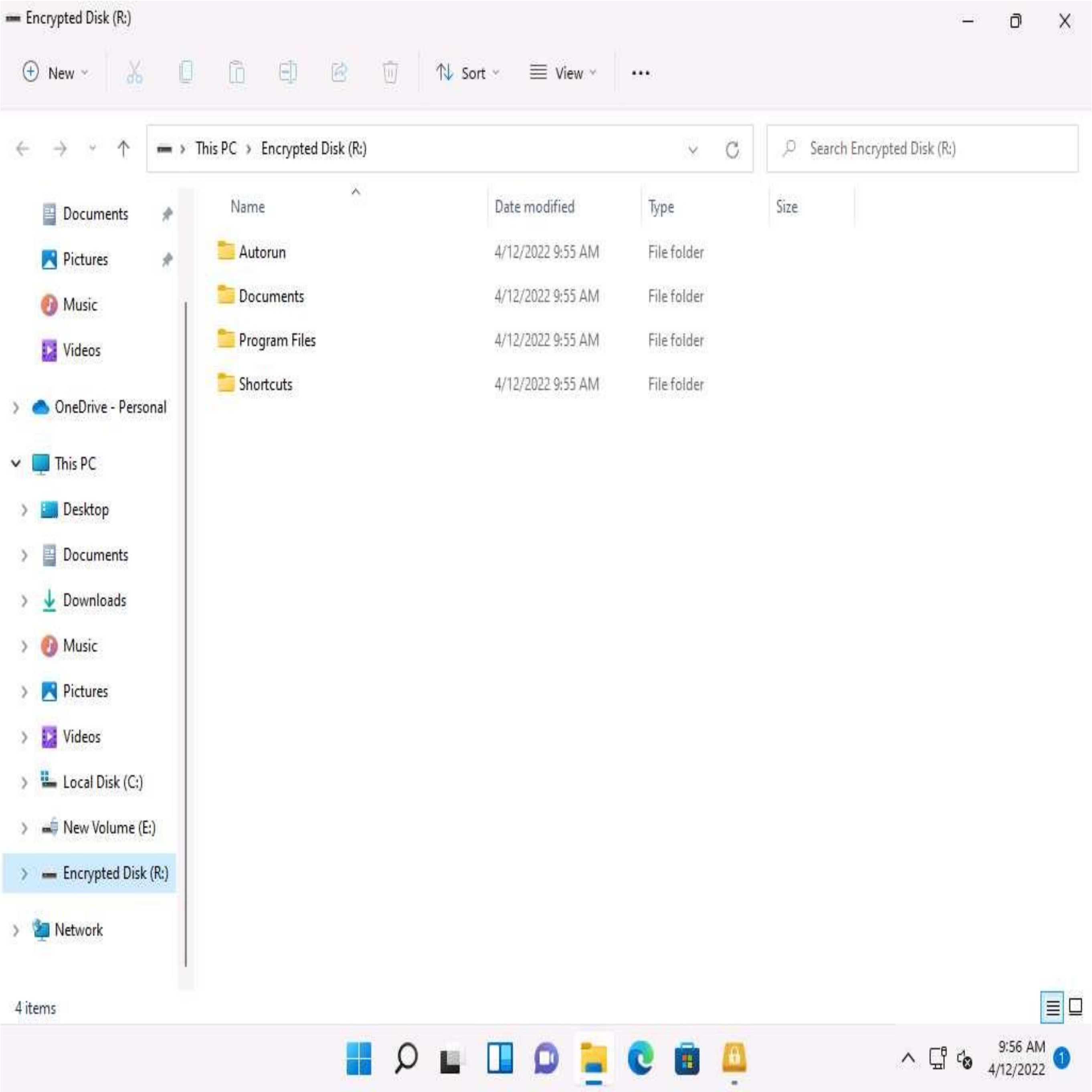
Specify a new password to access the disk: ••••••••

Confirm password: ••••••••

□ Make a shortcut to the disk on your desktop

10. □ Wait until the encrypted volume is created. The time to create the encrypted volume depends upon the size you specified under the **Disk Size** option: if large, it will take a long time to create the volume.

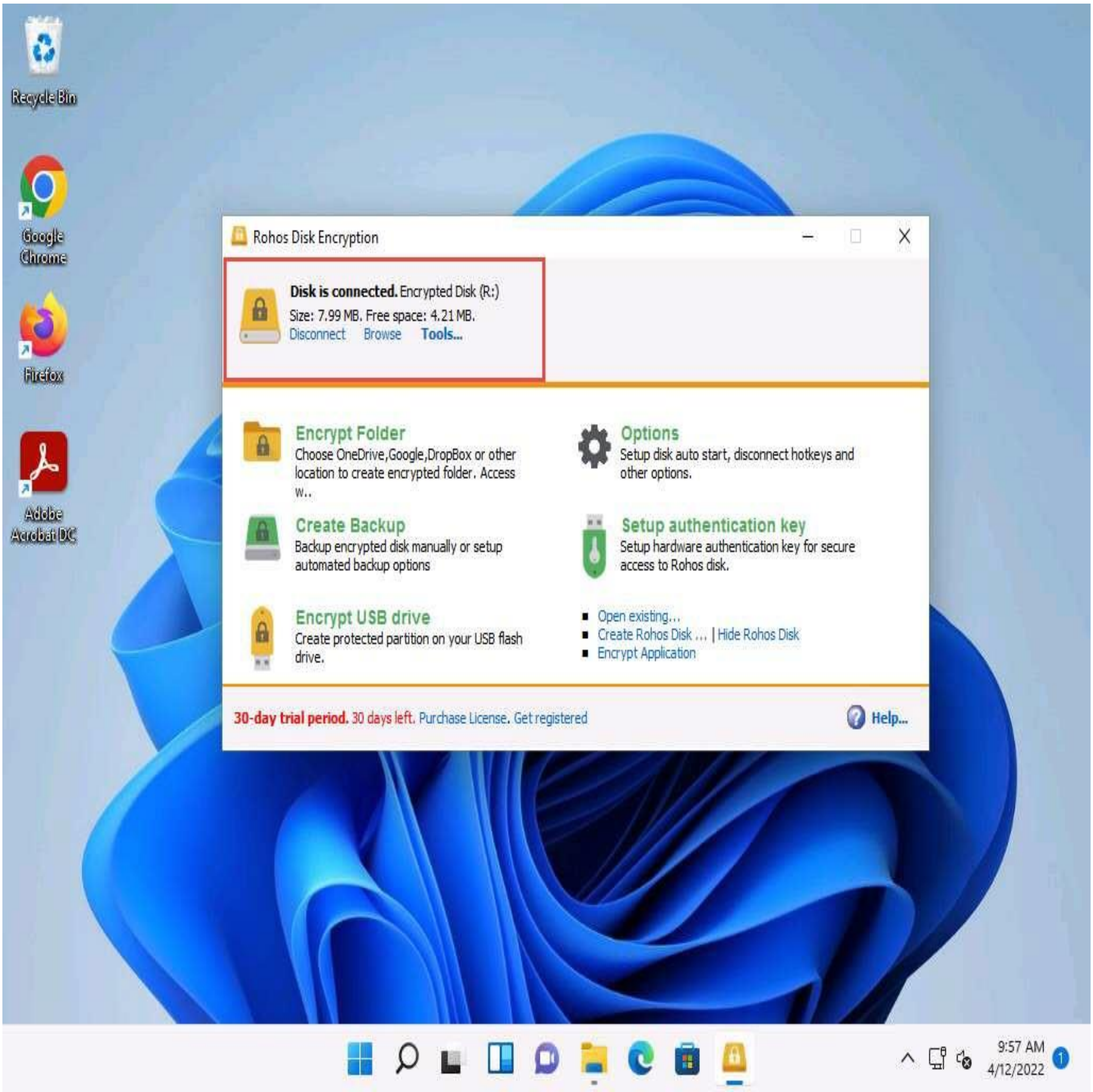
11. □ On creating the encrypted volume, the **Encrypted Disk (R:)** window appears, displaying the default disk content, as shown in the screenshot.



Name	Date modified	Type	Size
Autorun	4/12/2022 9:55 AM	File folder	
Documents	4/12/2022 9:55 AM	File folder	
Program Files	4/12/2022 9:55 AM	File folder	
Shortcuts	4/12/2022 9:55 AM	File folder	

12. □ The **Disk is connected** notification appears at the top section of the **Rohos Disk Encryption** window.

This drive appears only when you are connected to Rohos Disk Encryption, and disappears when you exit.



Disk is connected. Encrypted Disk (R:)

Size: 7.99 MB. Free space: 4.21 MB.

Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Setup disk auto start, disconnect hotkeys and other options.

Backup encrypted disk manually or setup automated backup options

Setup hardware authentication key for secure access to Rohos disk.

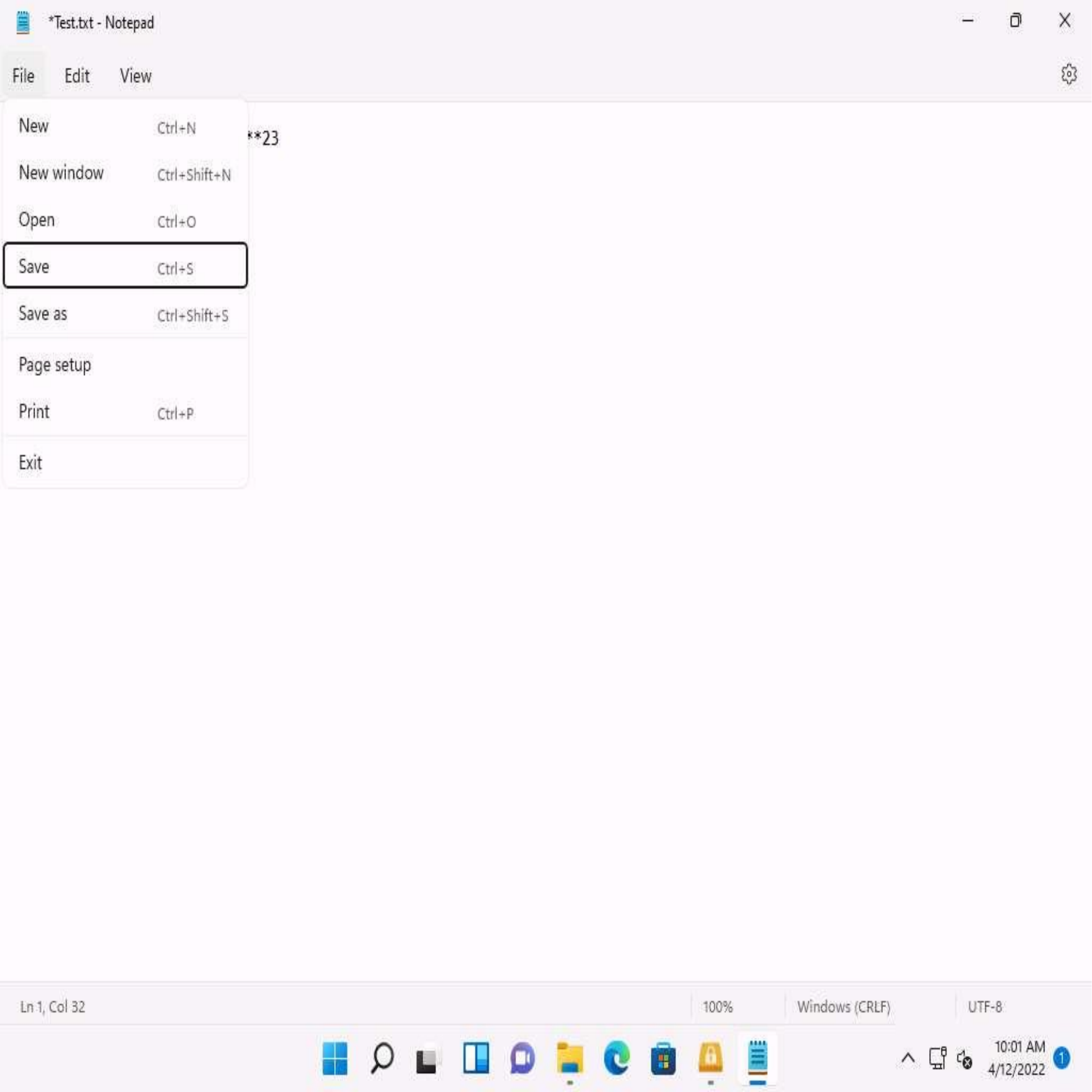
Create protected partition on your USB flash drive.

30-day trial period. 30 days left.

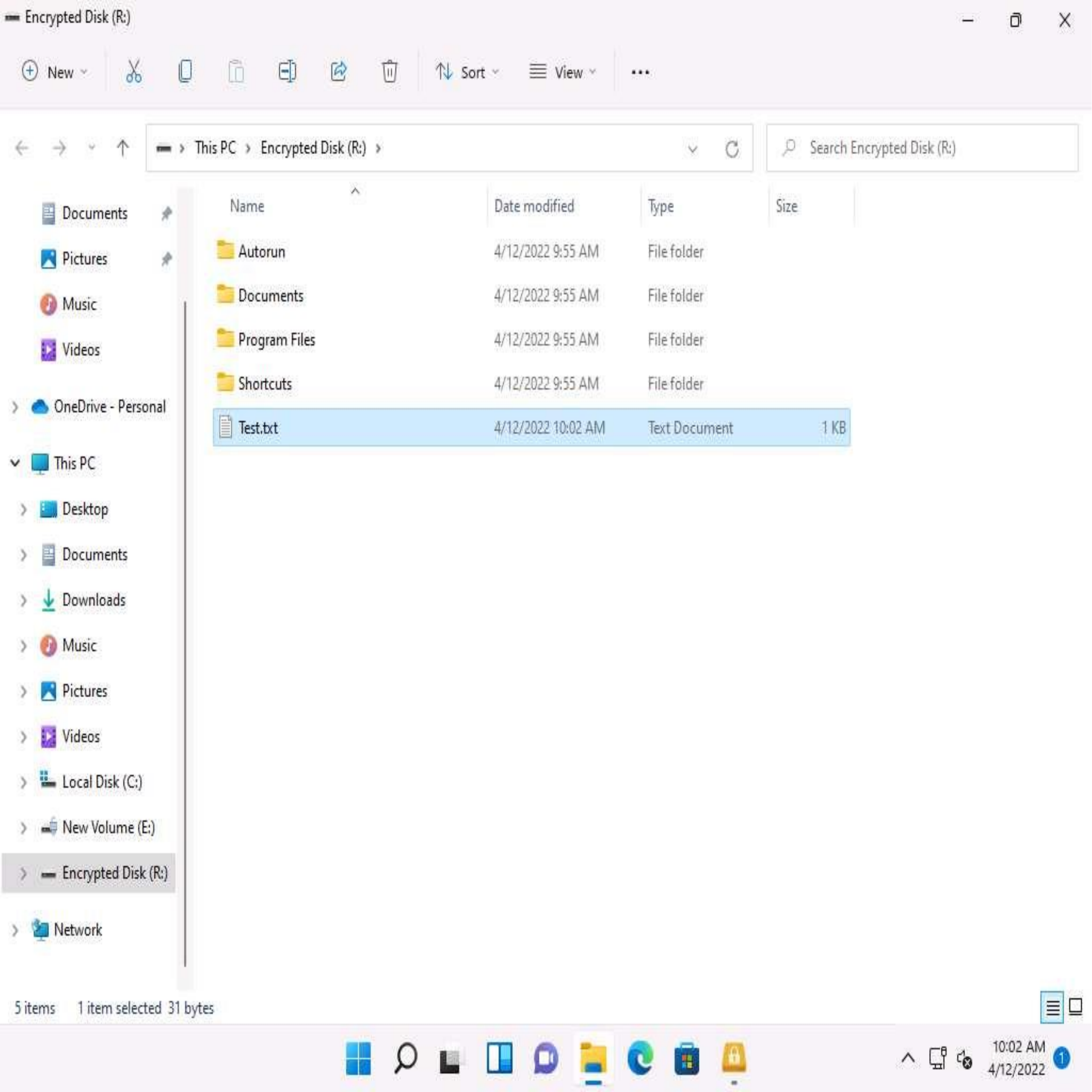
13. □ If you wish to conceal any important files/directories from anyone accessing your system, you can place them in this drive and access them whenever required (by launching Rohos and entering the password).

14. □ Now, we shall place a text file in **Encrypted disk (R:)**. To do so, create a text file on **Desktop** and name it **Test**. Open the file and insert text.

15. □ Click **File** in the menu bar and click **Save**.



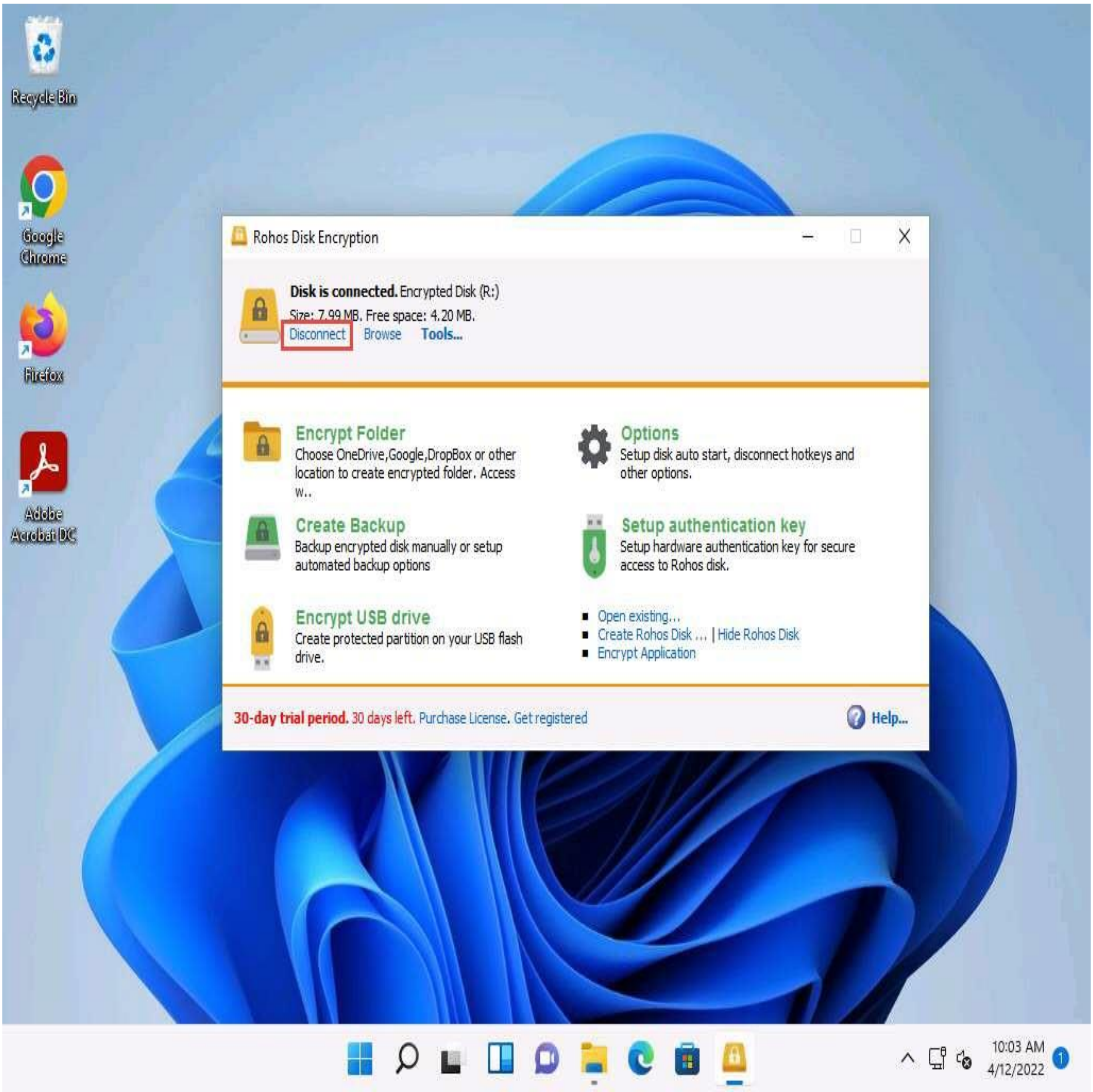
16. □ Copy the file from **Desktop** and paste into **Encrypted Disk (R:)**. Close the window.



Name	Date modified	Type	Size
Autorun	4/12/2022 9:55 AM	File folder	
Documents	4/12/2022 9:55 AM	File folder	
Program Files	4/12/2022 9:55 AM	File folder	
Shortcuts	4/12/2022 9:55 AM	File folder	
Test.txt	4/12/2022 10:02 AM	Text Document	1 KB

5 items 1 item selected 31 bytes

17. □ Switch to the **Rohos Disk Encryption** window and click **Disconnect** to dismount **Encrypted disk (R:)**.



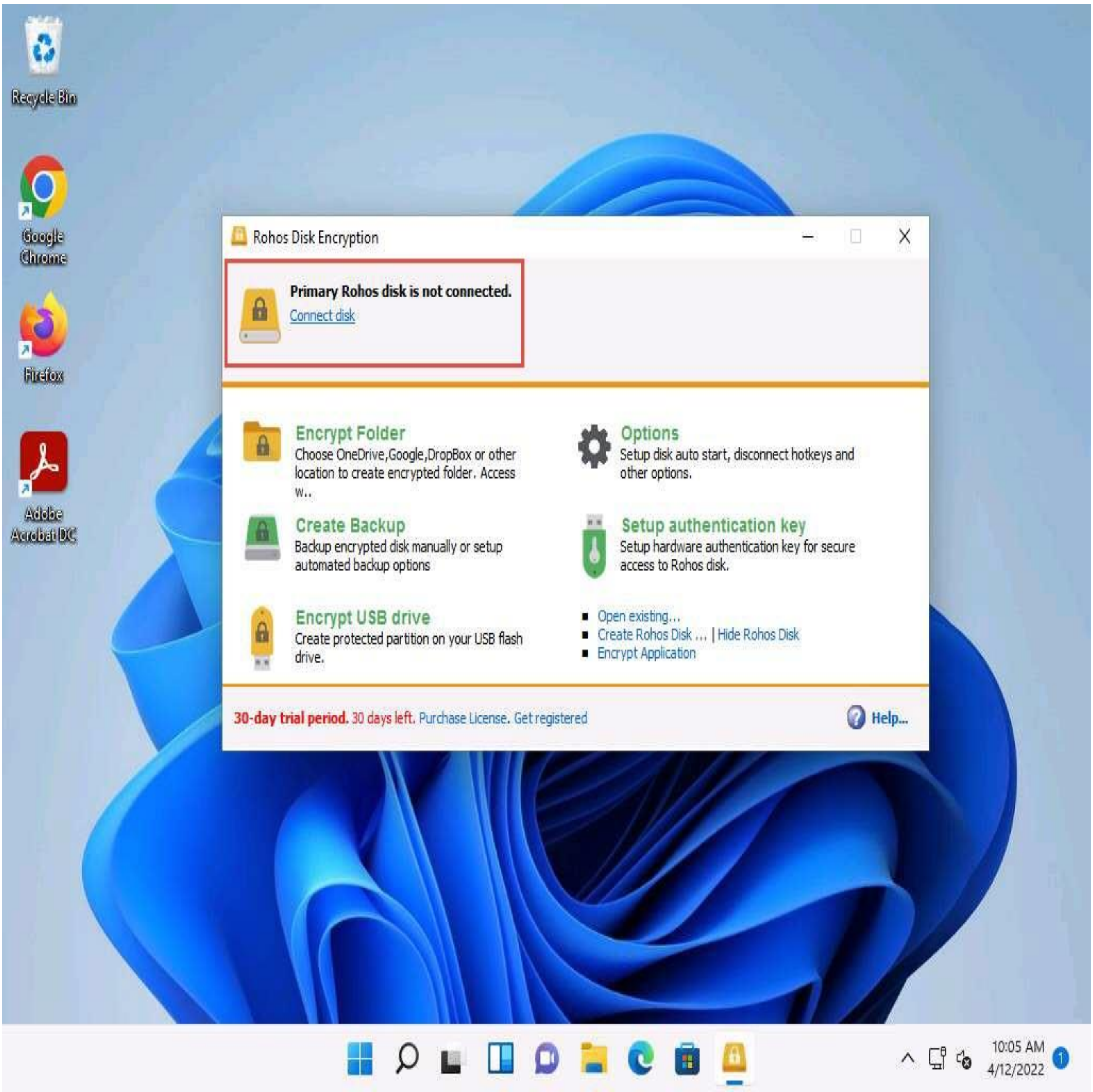
Rohos Disk Encryption

Disk is connected. Encrypted Disk (R:)

Size: 7.99 MB. Free space: 4.20 MB.

Recycle Bin
Google Chrome
Firefox
Adobe Acrobat DC
Disconnect
Browse
Tools...
Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..
Options
Setup disk auto start, disconnect hotkeys and other options.
Create Backup
Backup encrypted disk manually or setup automated backup options
Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.
Encrypt USB drive
Create protected partition on your USB flash drive.
Open existing...
Create Rohos Disk ... | Hide Rohos Disk
Encrypt Application
30-day trial period. 30 days left. Purchase License. Get registered
Help...
10:03 AM
4/12/2022

18. □ A notification appears stating **Primary Rohos disk is not connected** at the top of the **Rohos Disk Encryption** window. To mount the disk again, click the **Connect disk** option.



Rohos Disk Encryption

Primary Rohos disk is not connected.

Connect disk

Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Options
Setup disk auto start, disconnect hotkeys and other options.

Create Backup
Backup encrypted disk manually or setup automated backup options

Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.

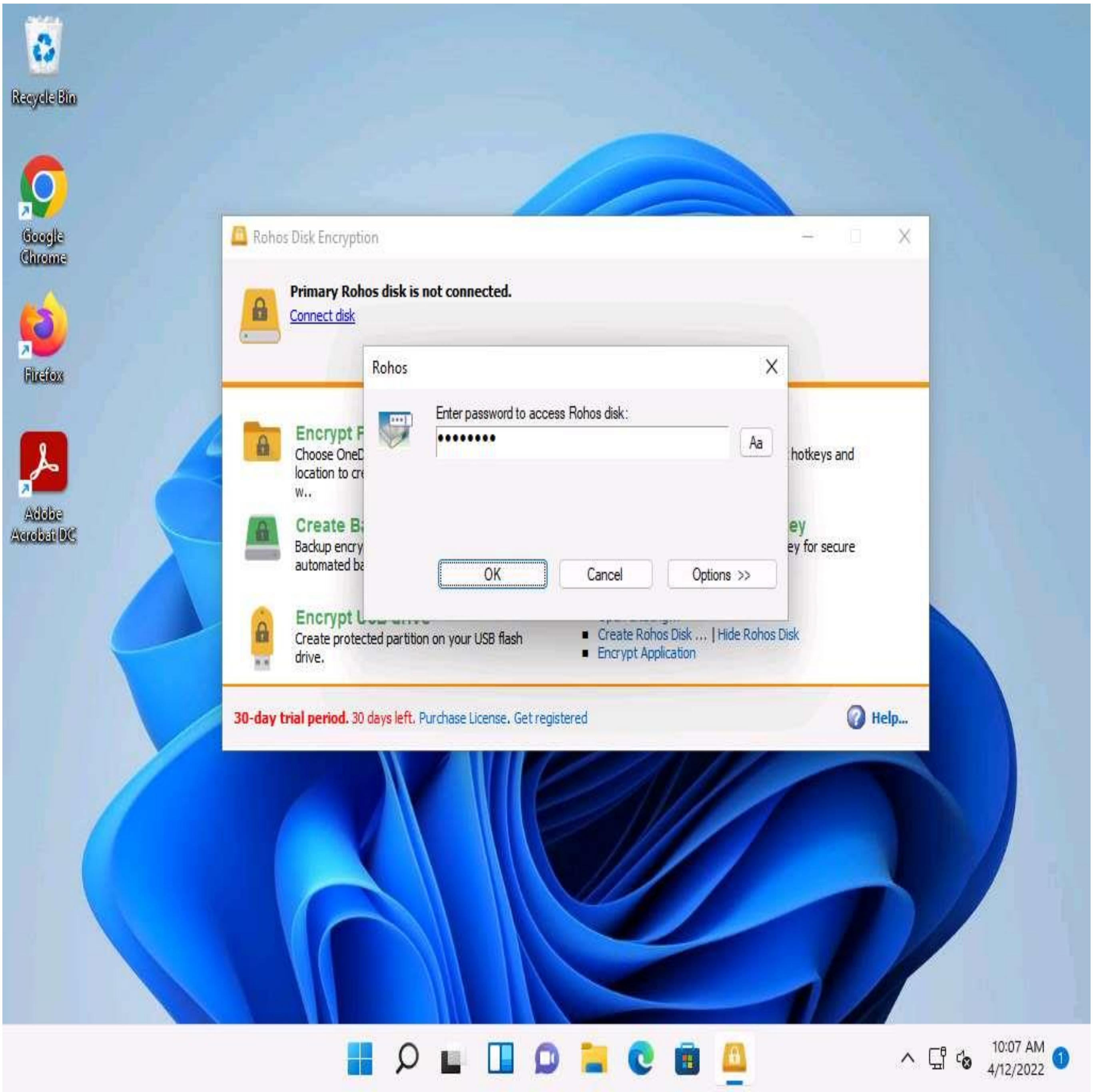
Encrypt USB drive
Create protected partition on your USB flash drive.

- Open existing...
- Create Rohos Disk ... | Hide Rohos Disk
- Encrypt Application

30-day trial period. 30 days left. Purchase License. Get registered

19. □ The **Rohos** pop-up appears; type the password you provided in **Step#6** into the **Enter password to access Rohos disk** field and click **OK**.

Here, the password is **test@123**.



Rohos Disk Encryption

Primary Rohos disk is not connected.

Connect disk

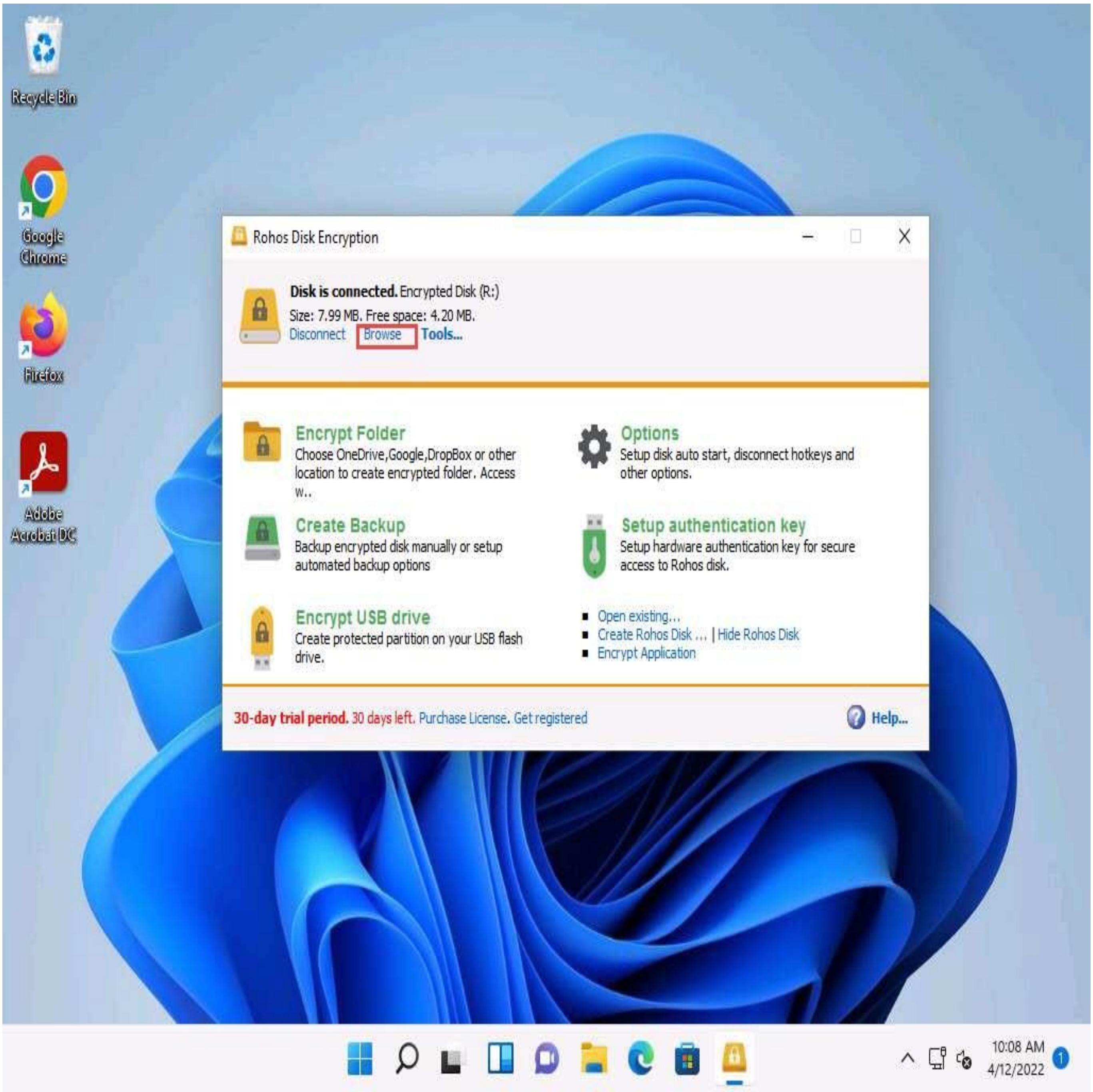
Rohos

Enter password to access Rohos disk:

••••••••

30-day trial period. 30 days left. Purchase License. Get registered

20. □ The **Disk is connected** notification appears in the **Rohos Disk Encryption** window. Click **Browse** to explore the disk content.



Disk is connected. Encrypted Disk (R:)

Size: 7.99 MB. Free space: 4.20 MB.

Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Options
Setup disk auto start, disconnect hotkeys and other options.

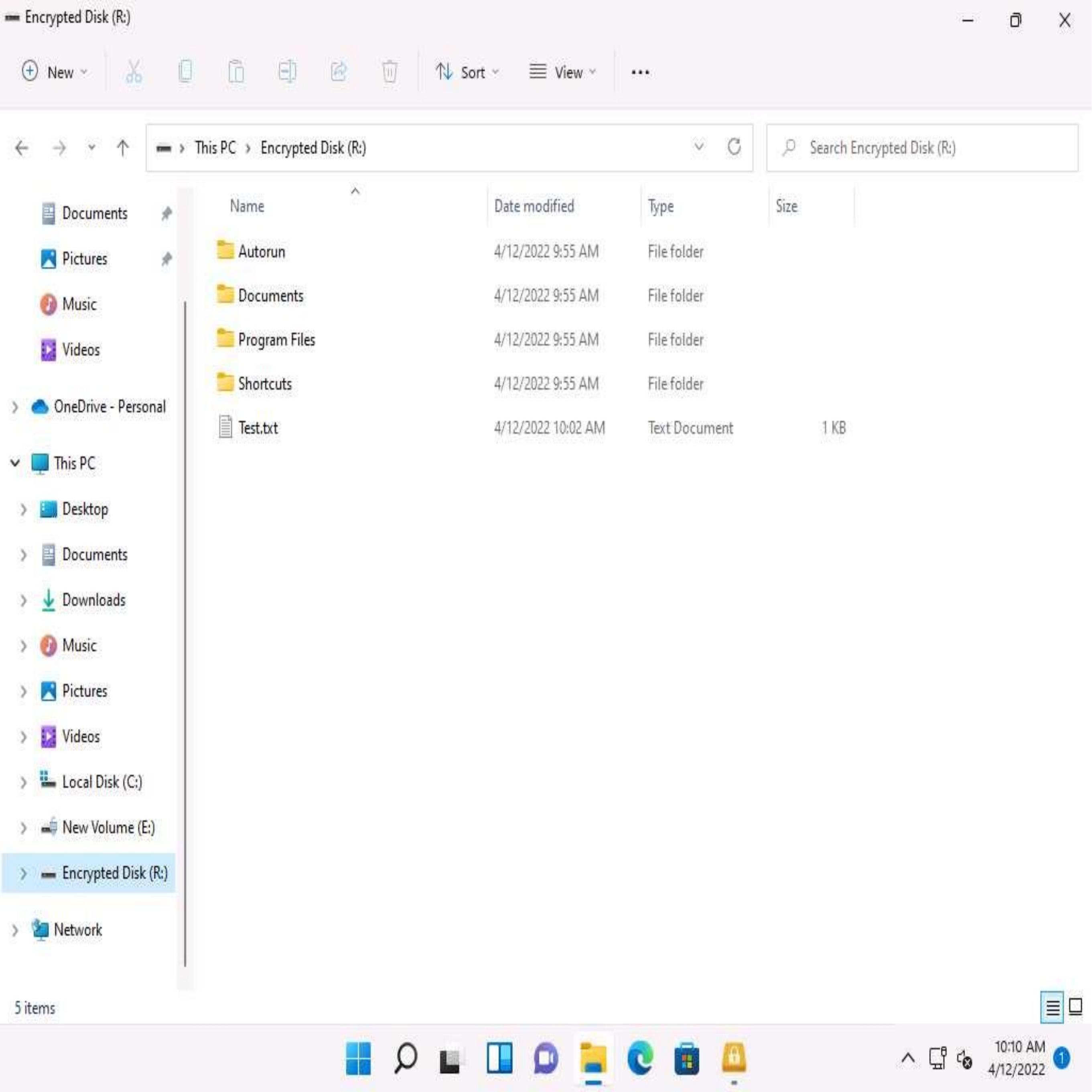
Create Backup
Backup encrypted disk manually or setup automated backup options

Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.

Encrypt USB drive
Create protected partition on your USB flash drive.

30-day trial period. 30 days left.

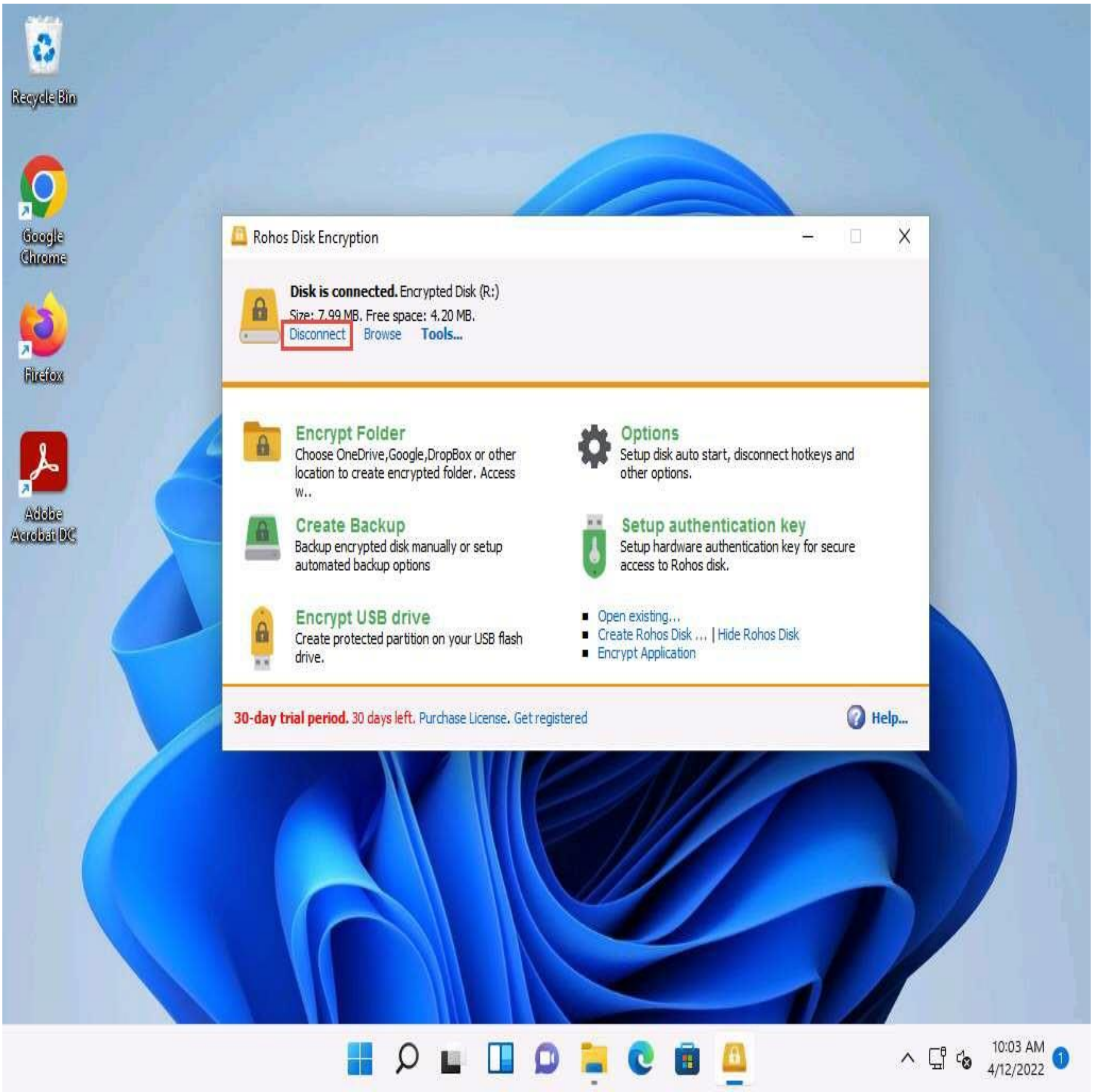
21. □ The **Encrypted Disk (R:)** window appears; you can see the **Test.txt** file that was pasted onto the disk earlier, as shown in the screenshot.



Name	Date modified	Type	Size
Autorun	4/12/2022 9:55 AM	File folder	
Documents	4/12/2022 9:55 AM	File folder	
Program Files	4/12/2022 9:55 AM	File folder	
Shortcuts	4/12/2022 9:55 AM	File folder	
Test.txt	4/12/2022 10:02 AM	Text Document	1 KB

5 items

22. □ You can access the disk content and further add, delete, and modify the files. After making the intended changes, click **Disconnect** again in the **Rohos Disk Encryption** window to dismount the disk.



Disk is connected. Encrypted Disk (R:)

Size: 7.99 MB. Free space: 4.20 MB.

Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Setup disk auto start, disconnect hotkeys and other options.

Backup encrypted disk manually or setup automated backup options

Setup hardware authentication key for secure access to Rohos disk.

Create protected partition on your USB flash drive.

30-day trial period. 30 days left.

You can also use the Encrypt USB drive option to share sensible information with someone via USB. You can use this application to store the files in an encrypted disk and share the password with that person. The person with whom you want to share the files can access them only after entering the correct password. This way, you can protect the files from being viewed by a third person and thereby safeguard them.

23. □ This concludes the demonstration of performing disk encryption using Rohos Disk Encryption.

24. □ You can also use other disk encryption tools such as **FinalCrypt** (http://www.finalcrypt.org), **Seqrite Encryption Manager** (https://www.seqrite.com), **FileVault** (https://support.apple.com), and **Gillsoft Full Disk Encryption** (http://www.gilisoft.com) to perform disk encryption.

25. □ Close all open windows and document all the acquired information