

Lab Assignment & Solution



Copyright © 1996–2021 HackerU Ltd.
All Rights Reserved.

Cybersecurity Professional Program

Microsoft Security

Microsoft Endpoint Security

MS-09-LS1

BitLocker

Note: Solutions for the instructor are shown inside the green box.

Lab Objective

Understand what drive encryption is and how to implement it on a Windows Server.

Lab Mission

Practice the installation and activation of BitLocker on a Windows Server 2016 machine.

Lab Duration

20–35 minutes

Requirements

- Basic working knowledge of Windows Server 2016
- Basic working knowledge of the Windows client
- Basic knowledge of BitLocker

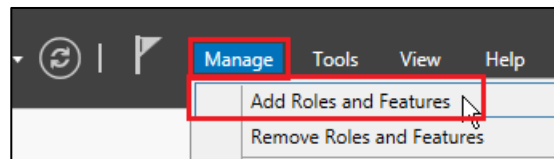
Resources

- Environment & Tools
 - VirtualBox
 - Windows Server 2016
 - Windows 10

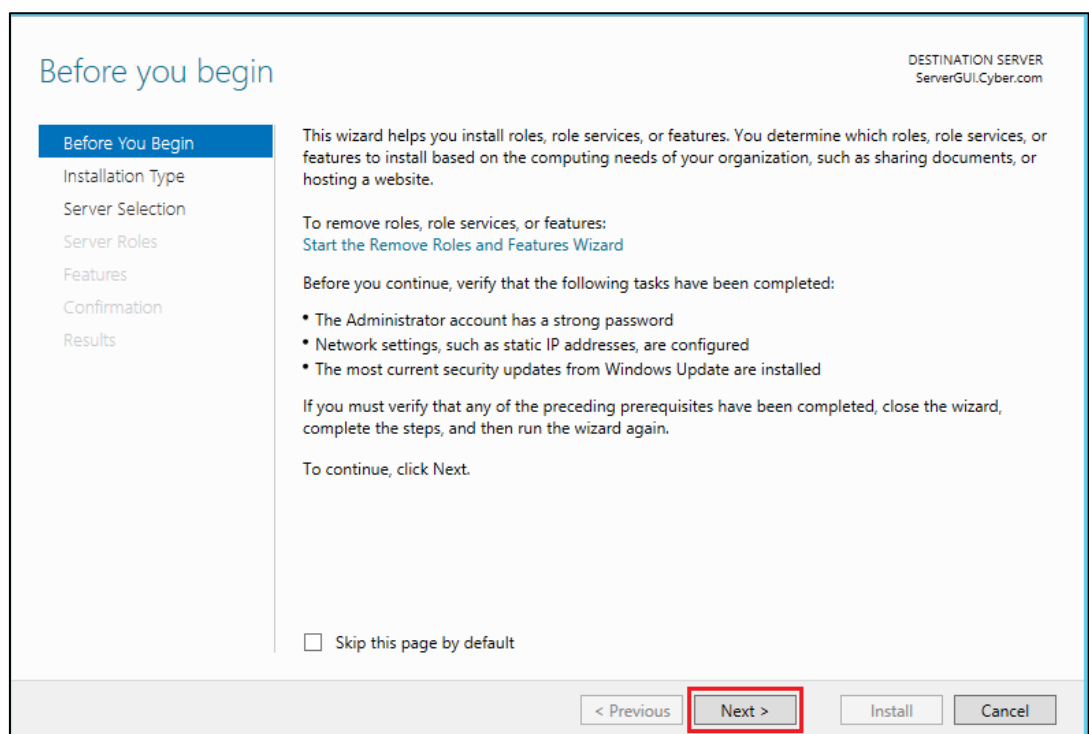
Lab Task 1: BitLocker Role Installation

In this task, you will install the BitLocker role on Server 1.

- 1 On the Server Manager dashboard, click the **Manage** drop-down menu and select **Add Roles and Features**.



- 2 On the first window, click **Next** to continue.



3 Select **Role-based** for the installation type.

The screenshot shows the 'Select installation type' window in the Destination Server GUI. The window has a title bar with 'DESTINATION SERVER' and 'ServerGUI.Cyber.com'. On the left is a navigation pane with the following items: 'Before You Begin', 'Installation Type' (highlighted in blue), 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the text: 'Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD)'. Below this text are two radio button options. The first option, 'Role-based or feature-based installation', is selected and its text is highlighted with a red rectangle. Below it is the text 'Configure a single server by adding roles, role services, and features.' The second option is 'Remote Desktop Services installation', which is unselected. Below it is the text 'Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.' At the bottom of the window are four buttons: '< Previous', 'Next >' (highlighted with a red rectangle), 'Install', and 'Cancel'.

Select installation type

DESTINATION SERVER
ServerGUI.Cyber.com

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous Next > Install Cancel

- 4 Select **server1.cyber.local** from the server pool to set the location where the feature will be installed.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. In the top right corner, it says 'DESTINATION SERVER: SERVER1.cyber.local'. On the left, a navigation pane lists the steps: 'Before You Begin', 'Installation Type', 'Server Selection' (which is highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the instruction 'Select a server or a virtual hard disk on which to install roles and features.' Below this are two radio buttons: 'Select a server from the server pool' (which is selected) and 'Select a virtual hard disk'. Under the 'Server Pool' section, there is a 'Filter:' text box. Below the filter is a table with three columns: 'Name', 'IP Address', and 'Operating System'. The table contains one row: 'SERVER1.cyber.local', '10.0.0.1', and 'Microsoft Windows Server 2016 Standard Evaluation'. Below the table, it says '1 Computer(s) found'. A paragraph of text explains that the page shows servers running Windows Server 2012 or newer, added via the 'Add Servers' command in Server Manager, and that offline servers and those with incomplete data collection are not shown. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

DESTINATION SERVER
SERVER1.cyber.local

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

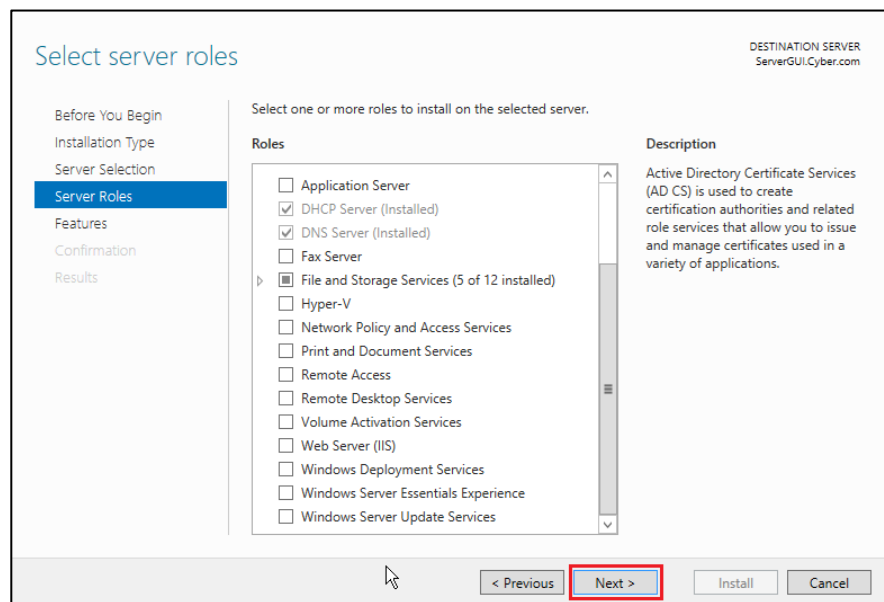
Name	IP Address	Operating System
SERVER1.cyber.local	10.0.0.1	Microsoft Windows Server 2016 Standard Evaluation

1 Computer(s) found

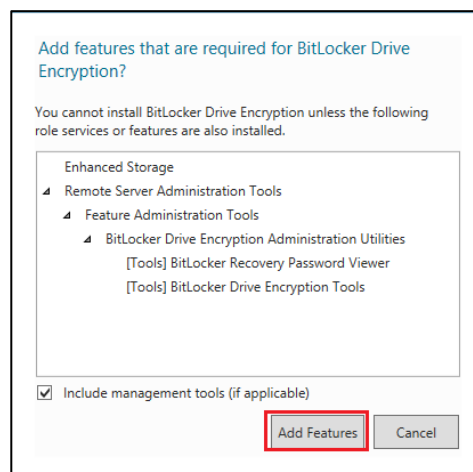
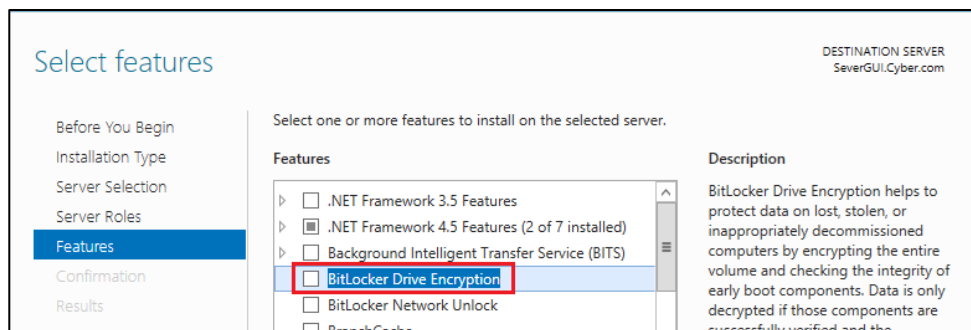
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous Next > Install Cancel

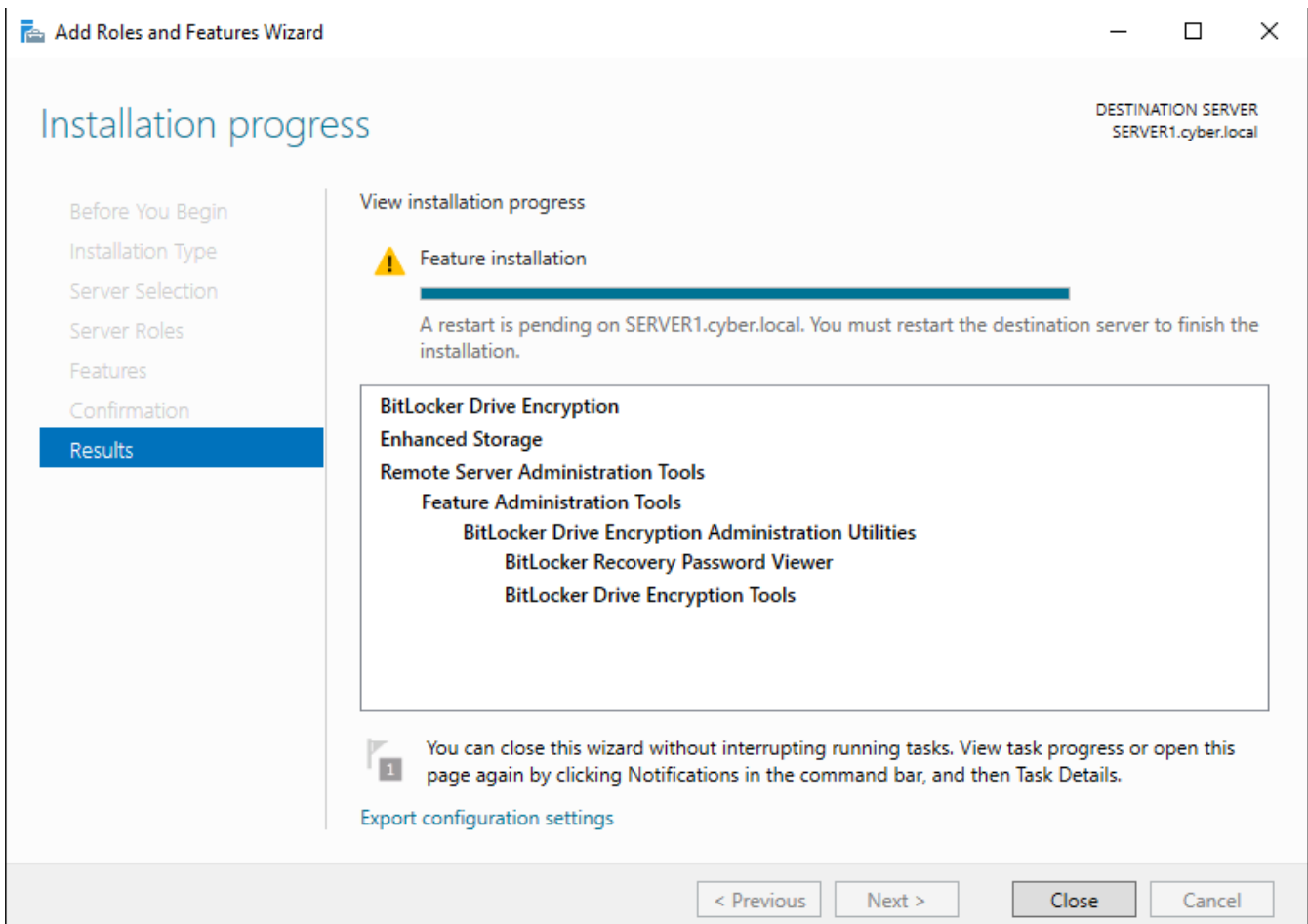
5 Skip the Server Roles step by clicking **Next**.



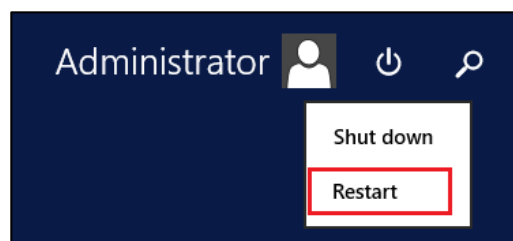
6 In the Features step, select **BitLocker Drive Encryption** and accept the configuration in the pop-up window. Then, click **Next**.



7 Click **Install** to begin the installation process.



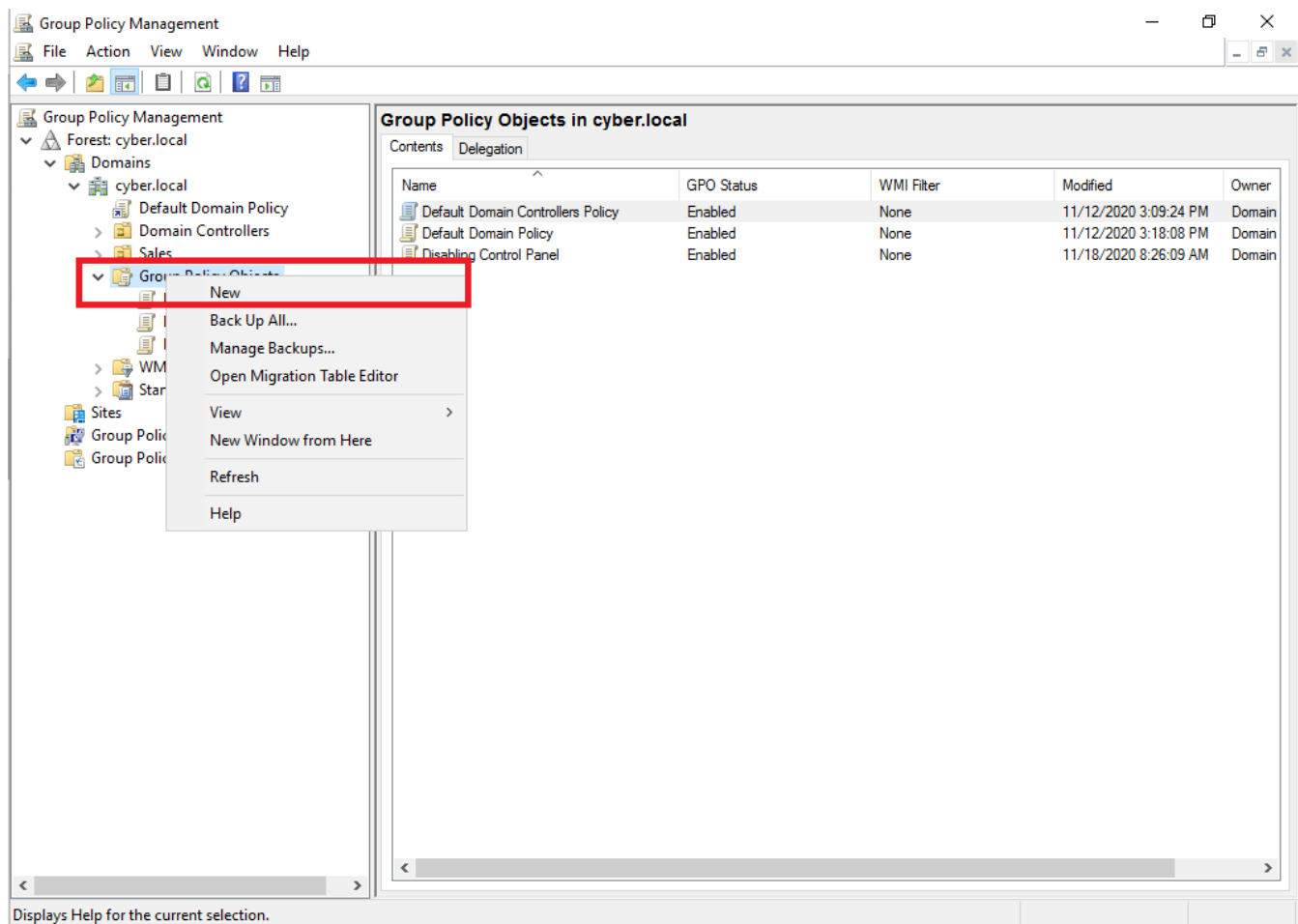
8 Finally, click **Start** on the bottom-left, and then click **Restart** in the top right corner.



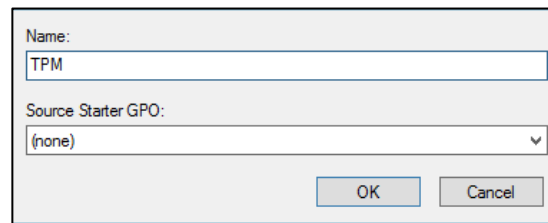
Lab Task 2: Authentication Without TPM

In this task, you will configure a policy for **BitLocker** to authenticate without a TPM chip, because the chip does not exist on the VM. Instead, it will request credentials on startup without using the TPM chip.

- 1 Open the **Group Policy Management** tool. Right-click **Group Policy Objects** and click **New** to create a new GPO.



- 2 Name the GPO **TPM** and click **OK**.

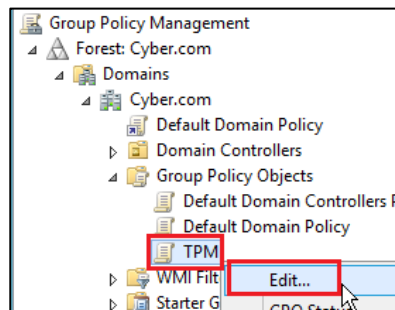


Name:
TPM

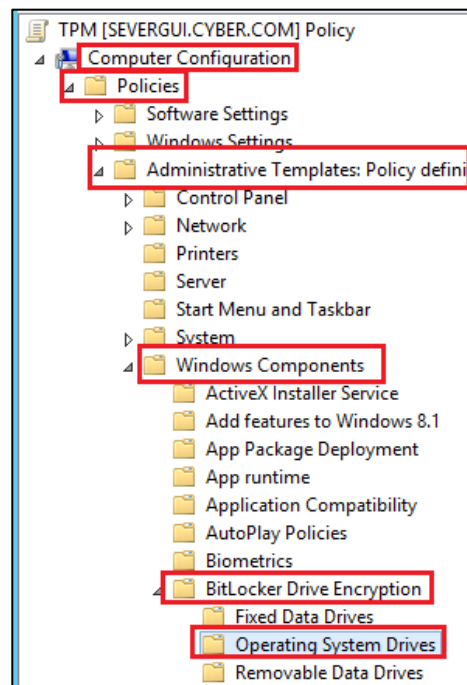
Source Starter GPO:
(none)

OK Cancel

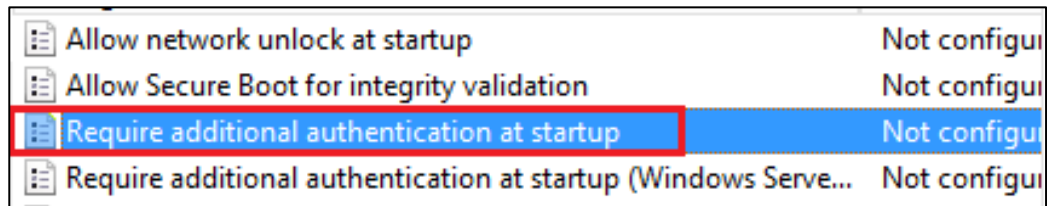
- 3 In **Group Policy Management**, right-click the **TPM** GPO and click **Edit...**.



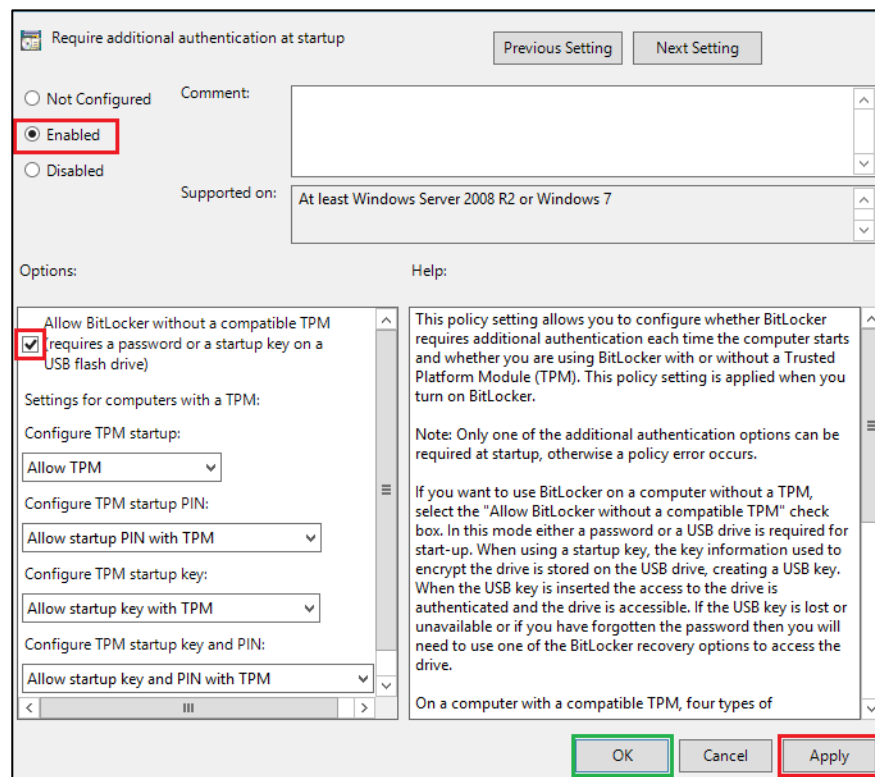
- 4 Navigate to **Operating System Drives** policies.



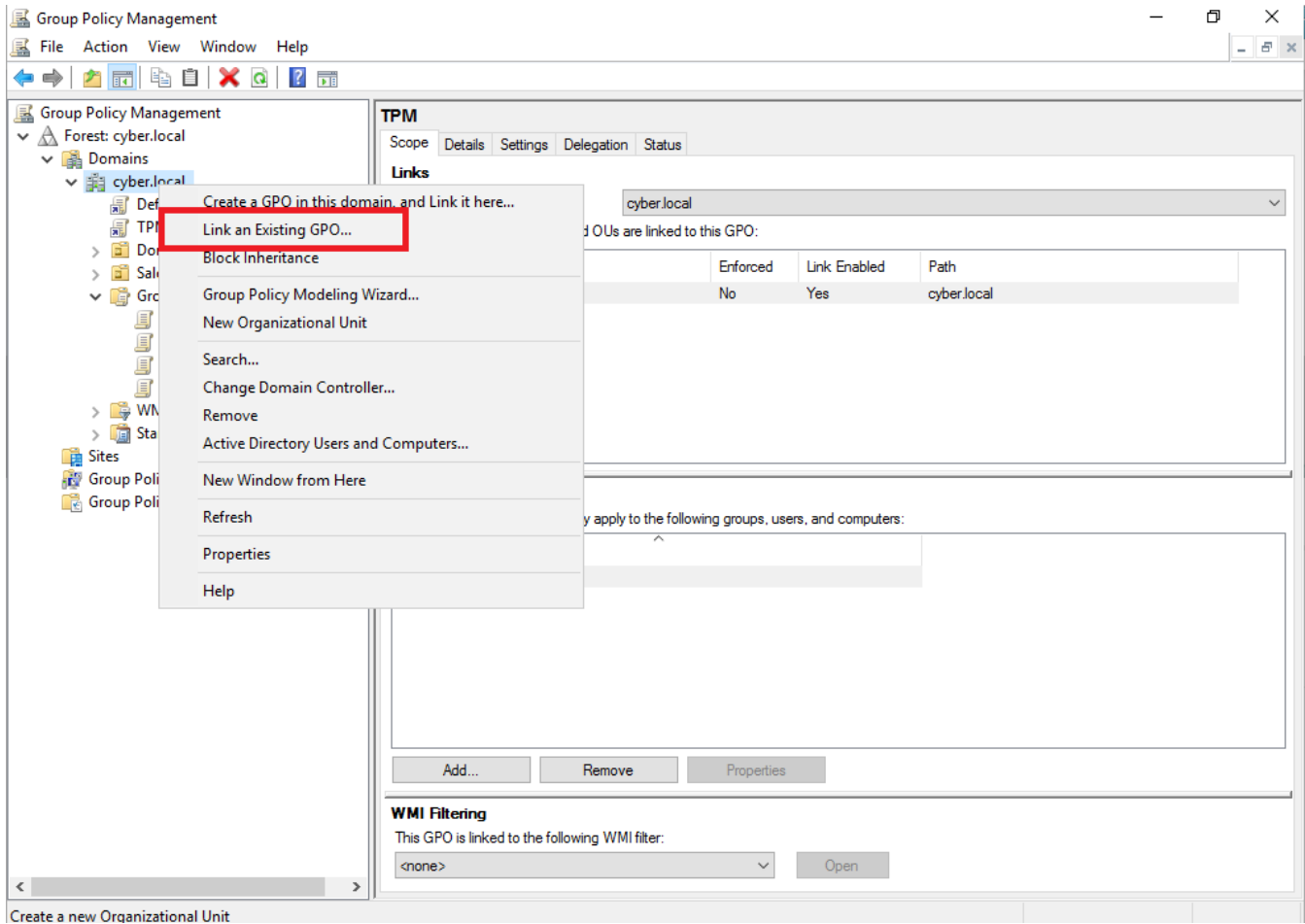
- 5 Open the setting called **Require additional authentication at startup**, set it to **Enabled**, and select **Allow BitLocker without...** Apply the settings for the policy and double-click **Require additional authentication at startup**.



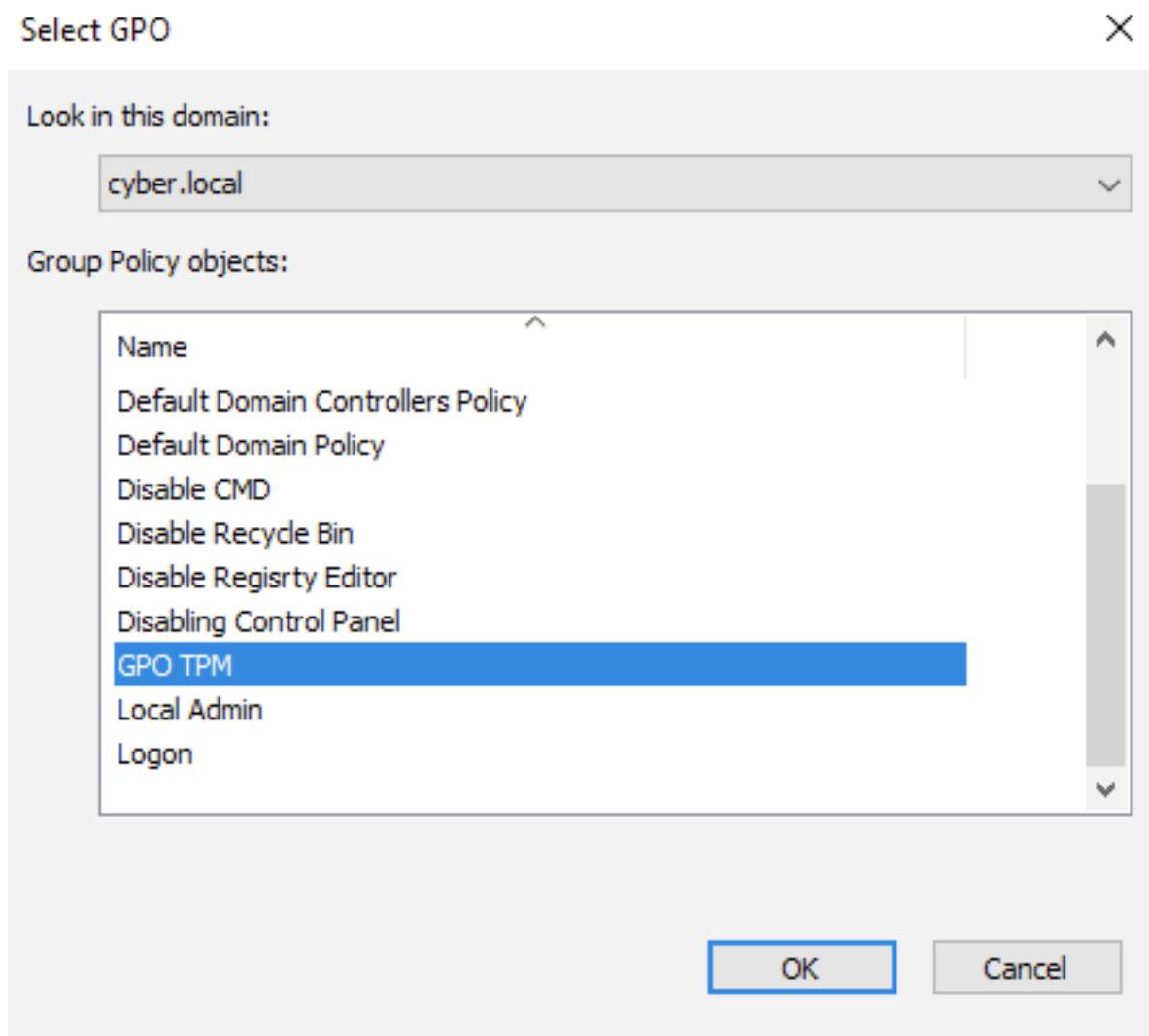
- 6 On the next window, click **Enabled** and select the option to require TPM to use a password. Then, click **Apply** and **OK**.



- 7 Link the GPO to the entire domain environment. Right-click the **cyber.local** domain and click **Link an Existing GPO...**



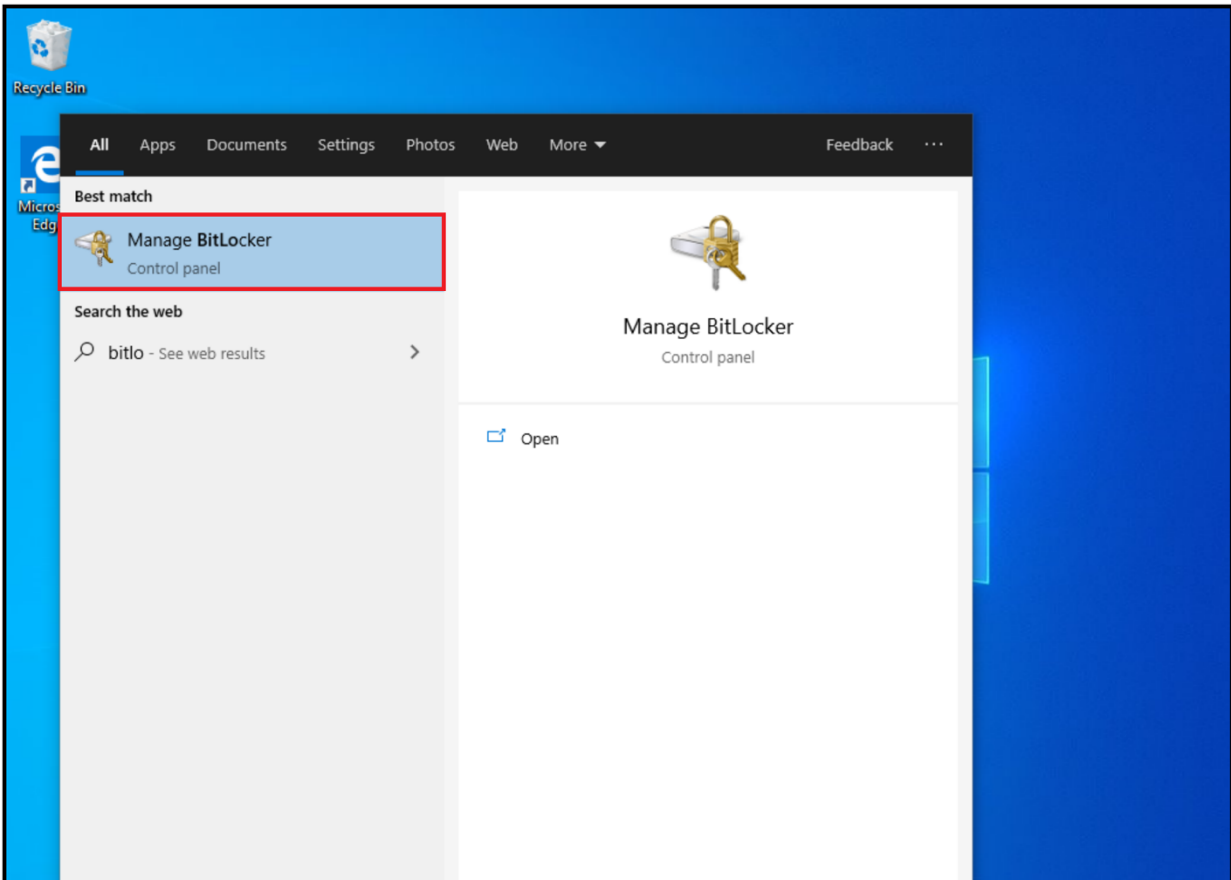
- 8 Click **GPO TPM** and **OK**.



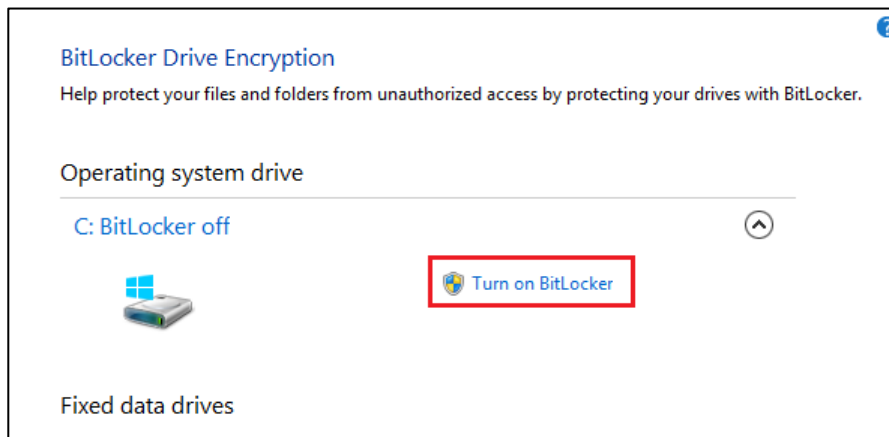
Lab Task 3: BitLocker Activation

In this task, you will activate **BitLocker** and use it to encrypt the C drive.

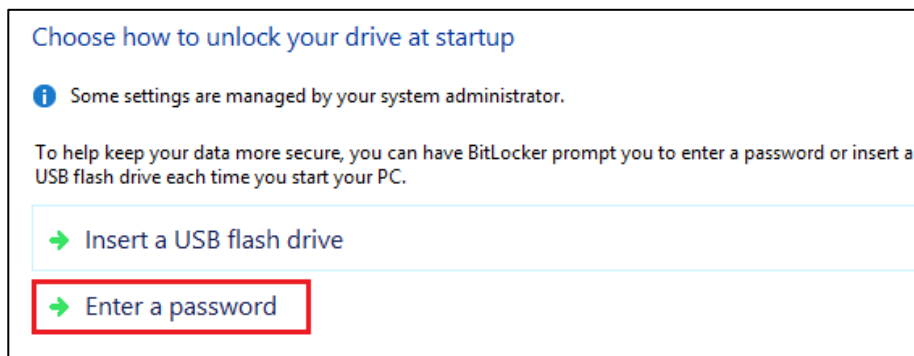
- 1 After the server restarts, go to your client-10 VM and click **Start** at the bottom right. Search for **BitLocker** and open **Manage BitLocker**.



- 2 In the window that appears, click **Turn on BitLocker**.



- 3 Select ***Enter a password***.



- 4 Enter **Pa\$\$w0rd** as the password. This will be used to unlock the drive. Then, click **Next**.

Create a password to unlock this drive

You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces.

Enter your password

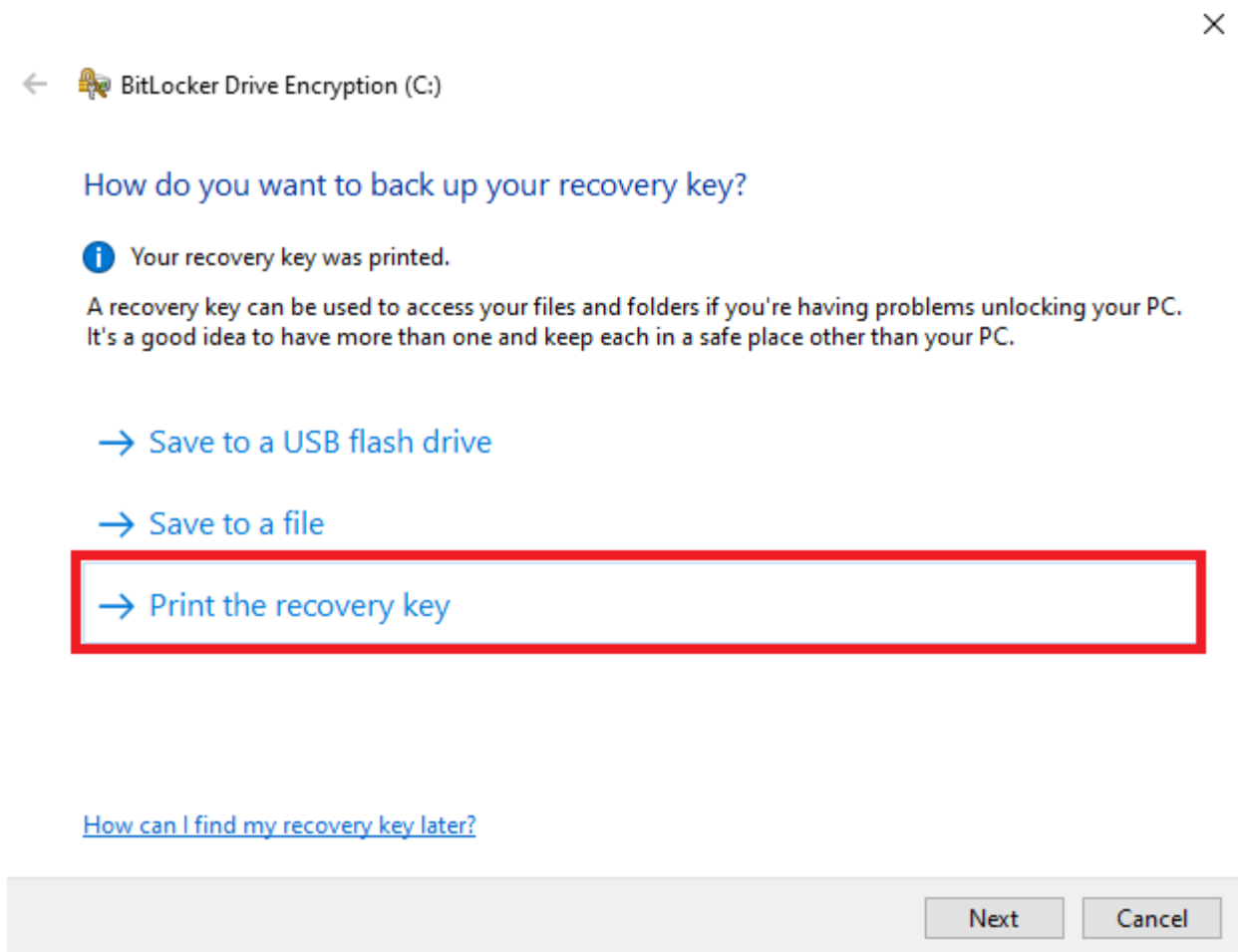
Reenter your password

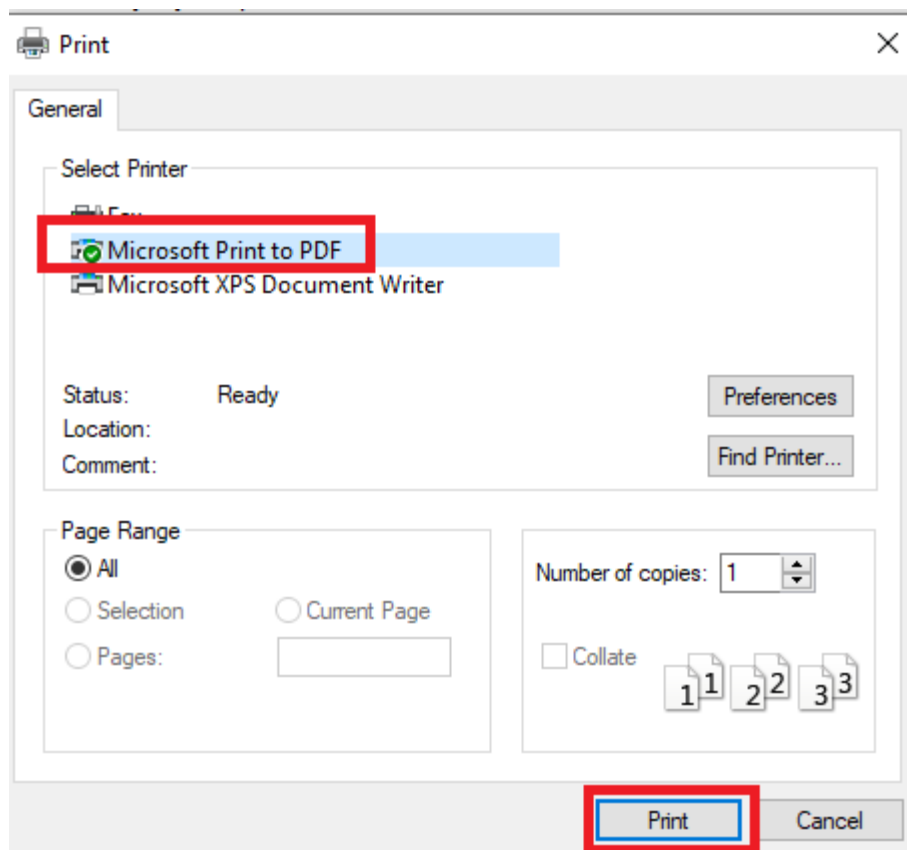
[Tips for creating a strong password.](#)

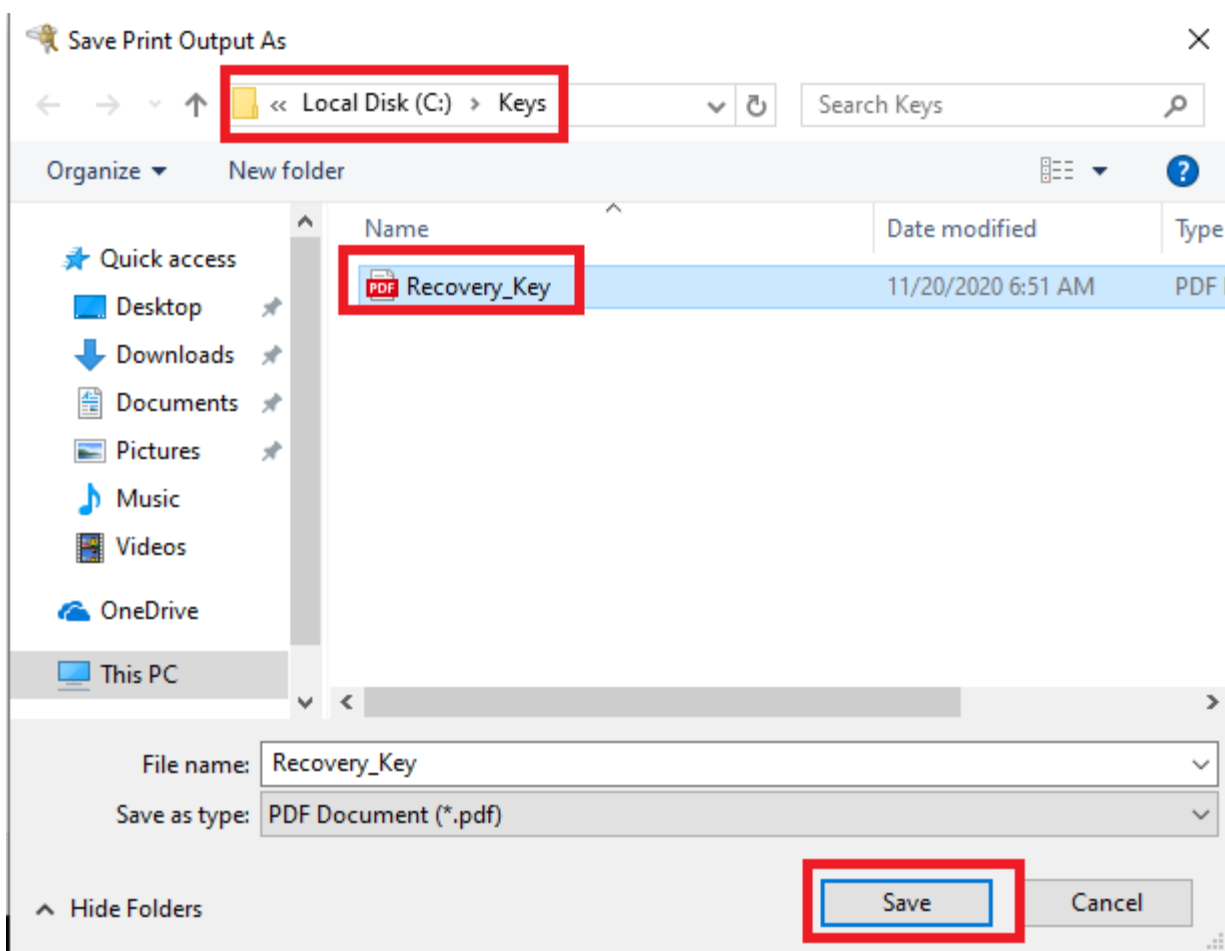
Next Cancel

- 5 Since the recovery key cannot be saved on the encrypted drive and because we have not attached a USB drive, we will work around the issue by printing our recovery key to PDF and saving it locally, as shown below.

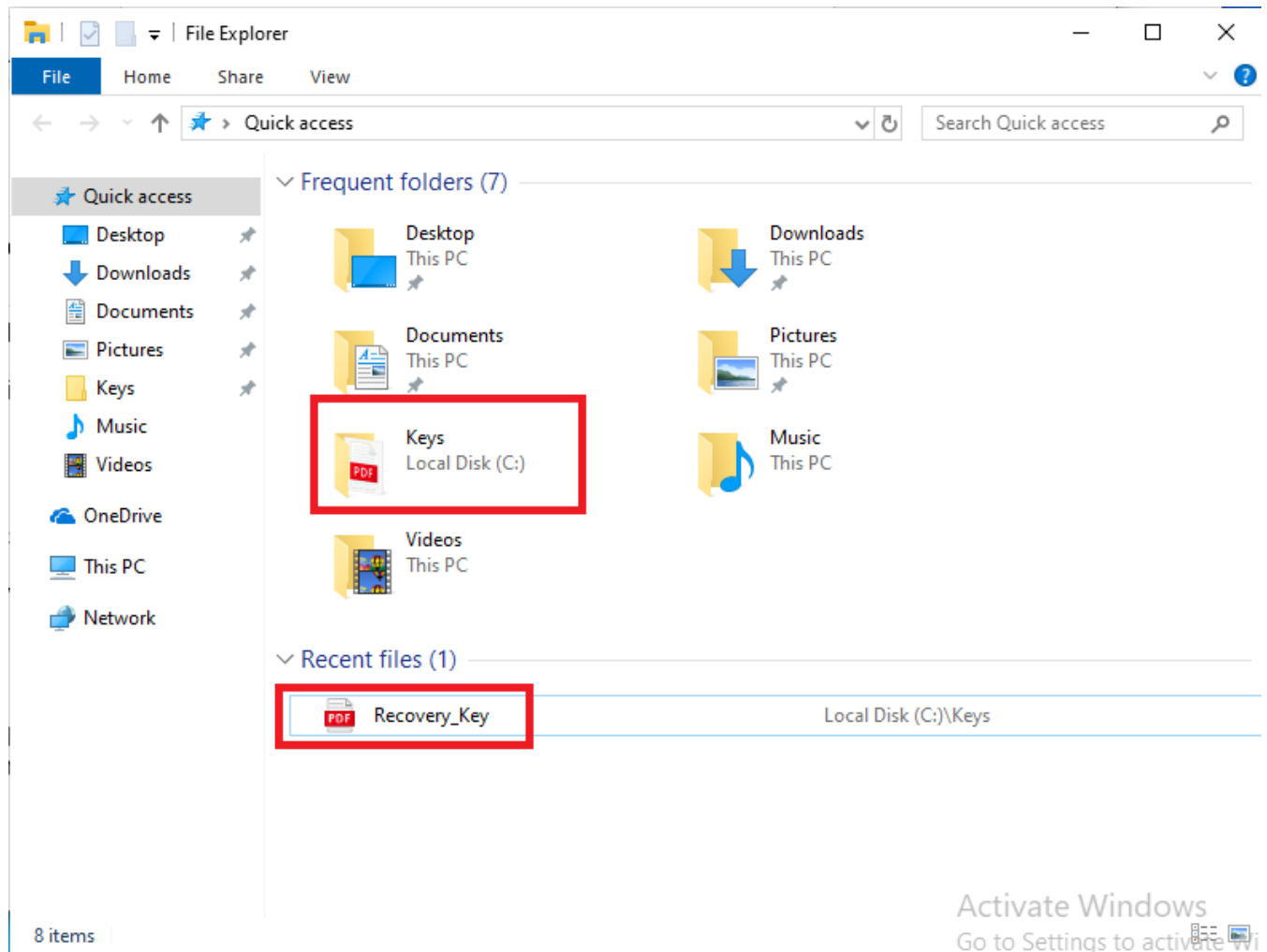
Note: Although not required for this lab, it is good practice to copy/paste the key to a secure location using the Share Clipboard feature and securely delete the **Keys** folder. However, it is not required for the functionality of the lab.

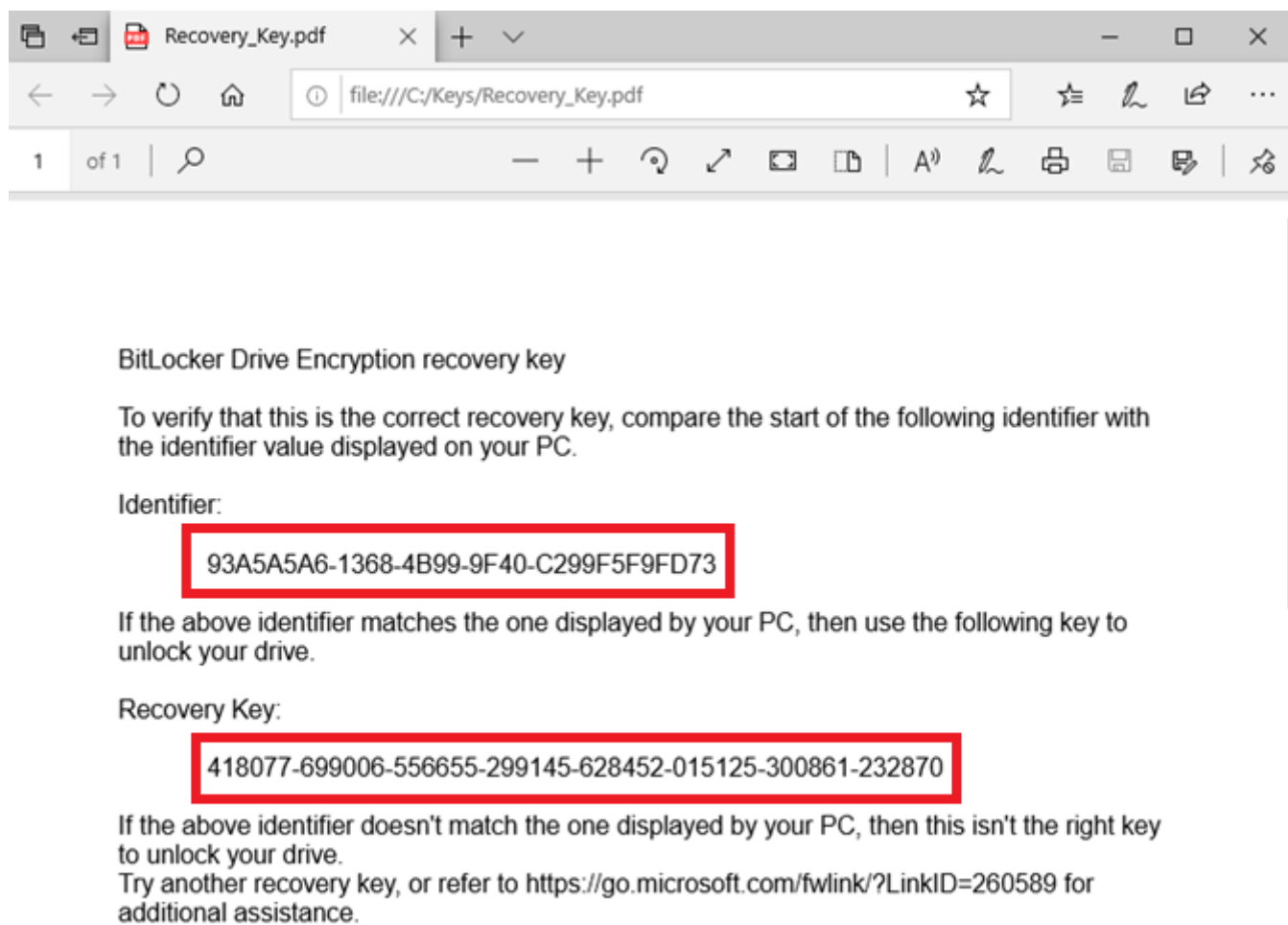




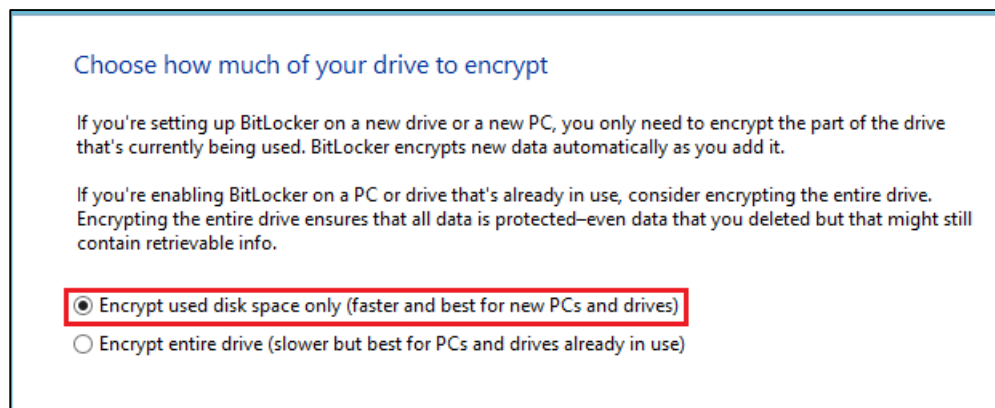


- 6 Open the recovery key located in **C:\Keys** by double-clicking the PDF file you just printed. As noted previously, you can copy this information to a more secure location if you wish, but it is not required for the functionality of this lab.

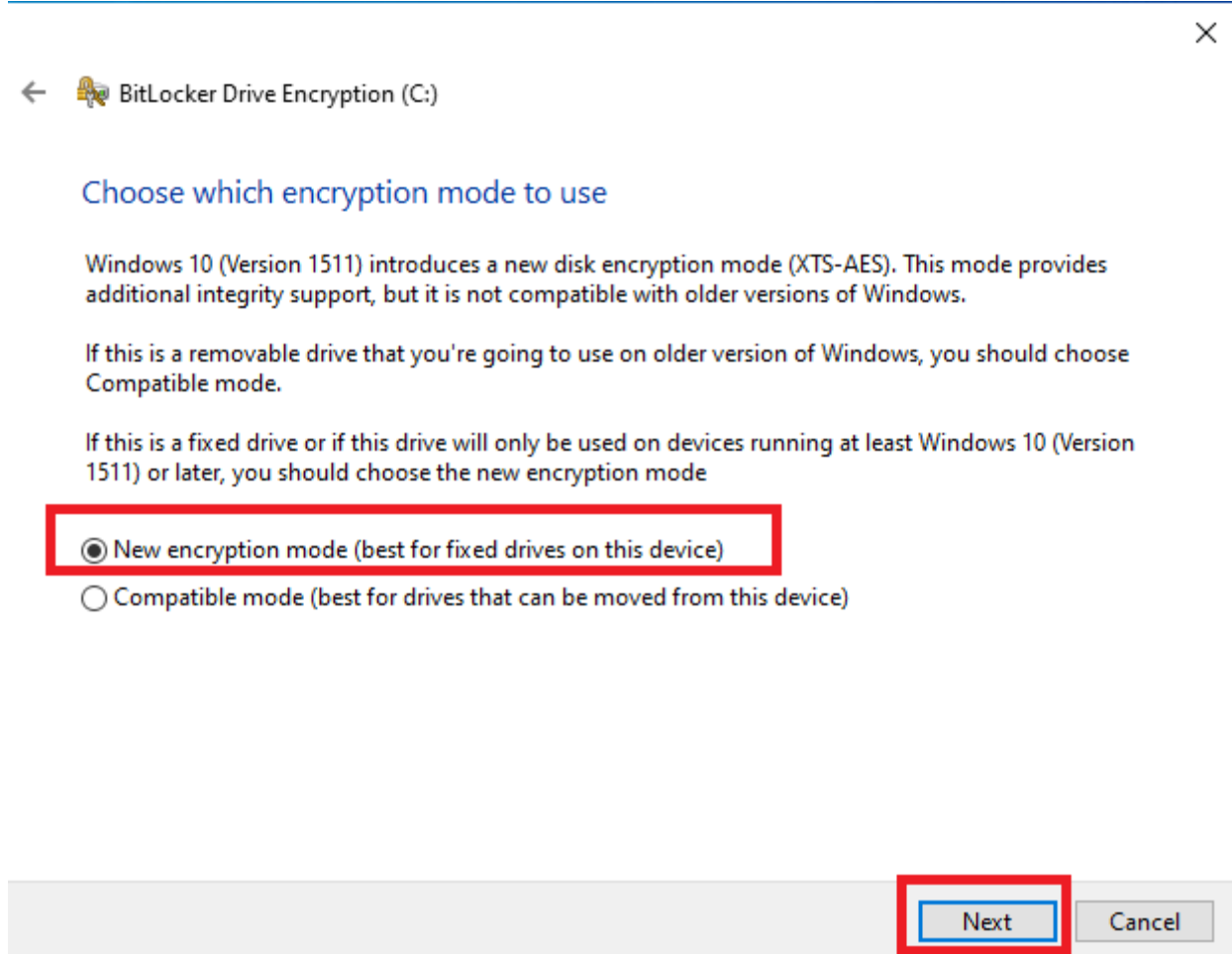




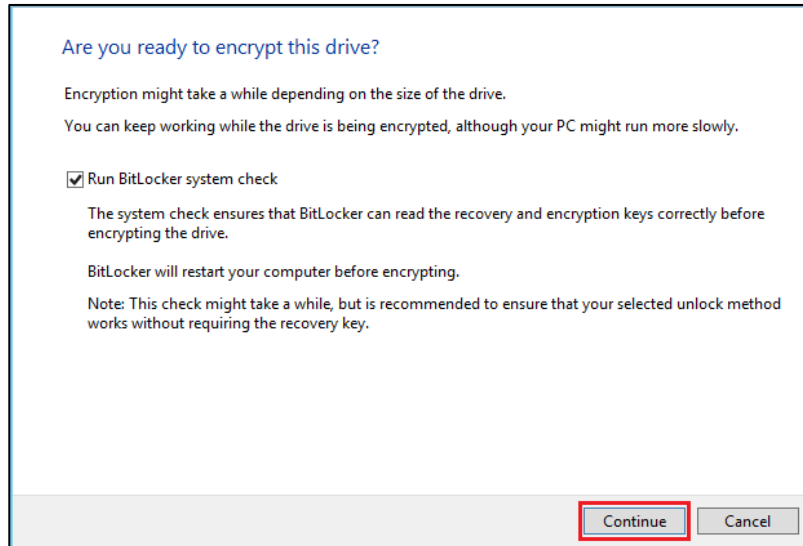
- 7 Click **Next** on the BitLocker Drive Encryption window, select **Encrypt used disk space only**, and click **Next**.



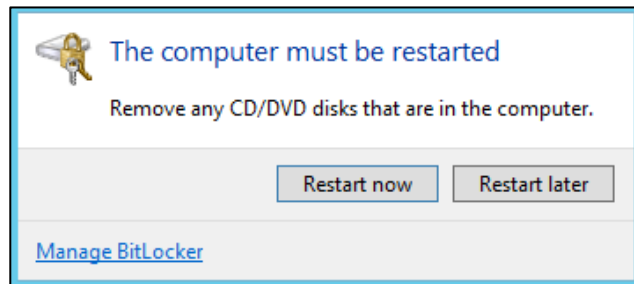
- 8 When prompted, choose **New encryption mode** (as shown below) and click **Next**.



- 9 On the next window, make sure **Run BitLocker system check** is selected and click **Continue**.



- 10 You will be notified that the computer will require restart. Restart the system to begin the encryption.
- Note:** The following window will appear if you have anything on your virtual disk drive. Eject the disk from the virtual drive and click **Restart now**.



- 11 Upon reboot and due to the enabled policy, your system is now encrypted. You will be prompted for a password, as shown below. Enter your password.

Note: You will not be using this configuration in the following labs and can turn off BitLocker when you are done with the lab if you wish.

