Title: **BitLocker Disk Encryption: Step-by-Step Implementation Using TPM 2.0 and USB**

Full Name: **Ali Huseynli**

Field: **Cybersecurity**

Date: **08.01.2026**

Introduction:

What Is BitLocker?

BitLocker is a Windows security feature designed to protect data by encrypting entire disks. It is commonly used to prevent unauthorized access to sensitive information in cases where a device is lost or stolen. By encrypting the disk, BitLocker ensures that data remains inaccessible without proper authentication, even if the storage device is removed and connected to another system.

Why Is Disk Encryption Important?

Without disk encryption, anyone with physical access to a device can bypass operating system protections and access personal or confidential data. Tools such as Sergei Strelec, Hiren's Boot, or similar bootable environments can be used to reset Windows passwords or directly access files, regardless of how strong the original password is. Disk encryption protects against these offline attacks by ensuring that data remains unreadable without the correct encryption key.

Purpose of This Lab

The purpose of this lab is to learn how to enable and configure BitLocker in different scenarios:

- On computers with TPM 2.0
- On computers without TPM
- On USB flash drives

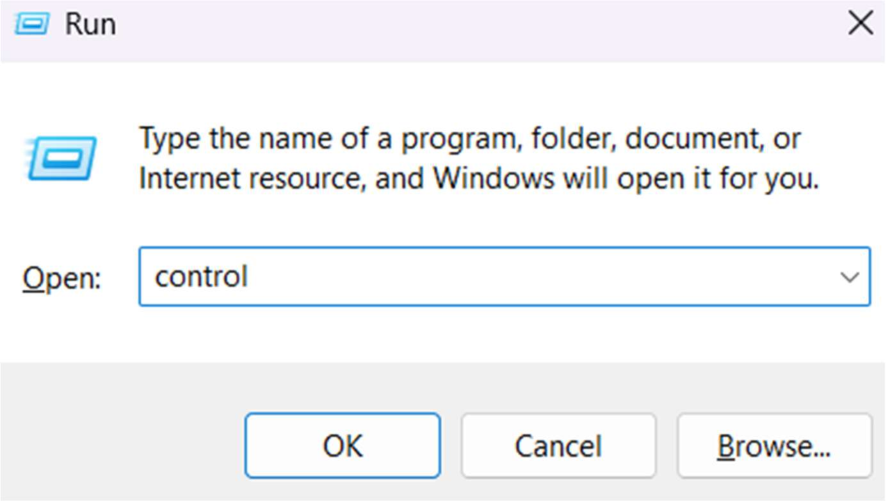
This practical exercise demonstrates how BitLocker enhances data security under various hardware and configuration conditions.

Requirements

- Windows 10/11 Pro
- TPM 2.0 (optional)
- USB Flash Drive
- Admin access

Scenario 1: BitLocker with TPM 2.0

1. **Press Win + R, type control, and press Enter.**

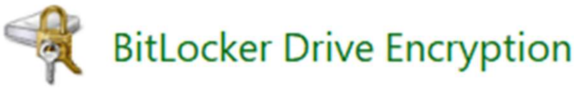


Run

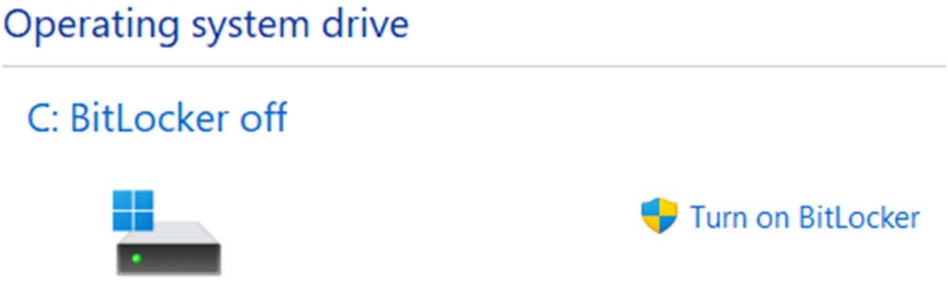
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: control

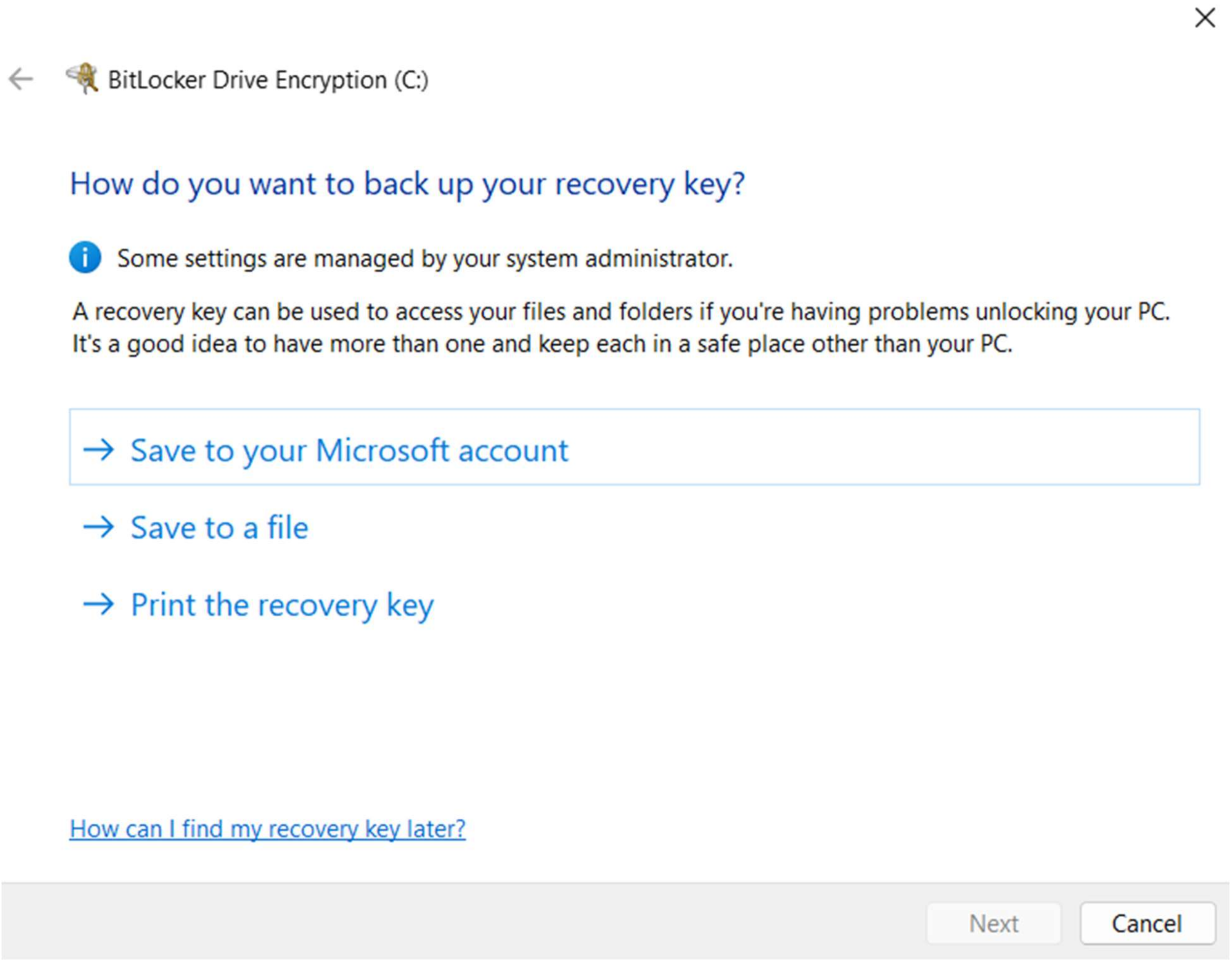
2. **Open *BitLocker Drive Encryption* from the Control Panel.**



3. **Click on *Turn on BitLocker*.**



4. **Here, you can choose how to back up your recovery key.**



BitLocker Drive Encryption (C:)

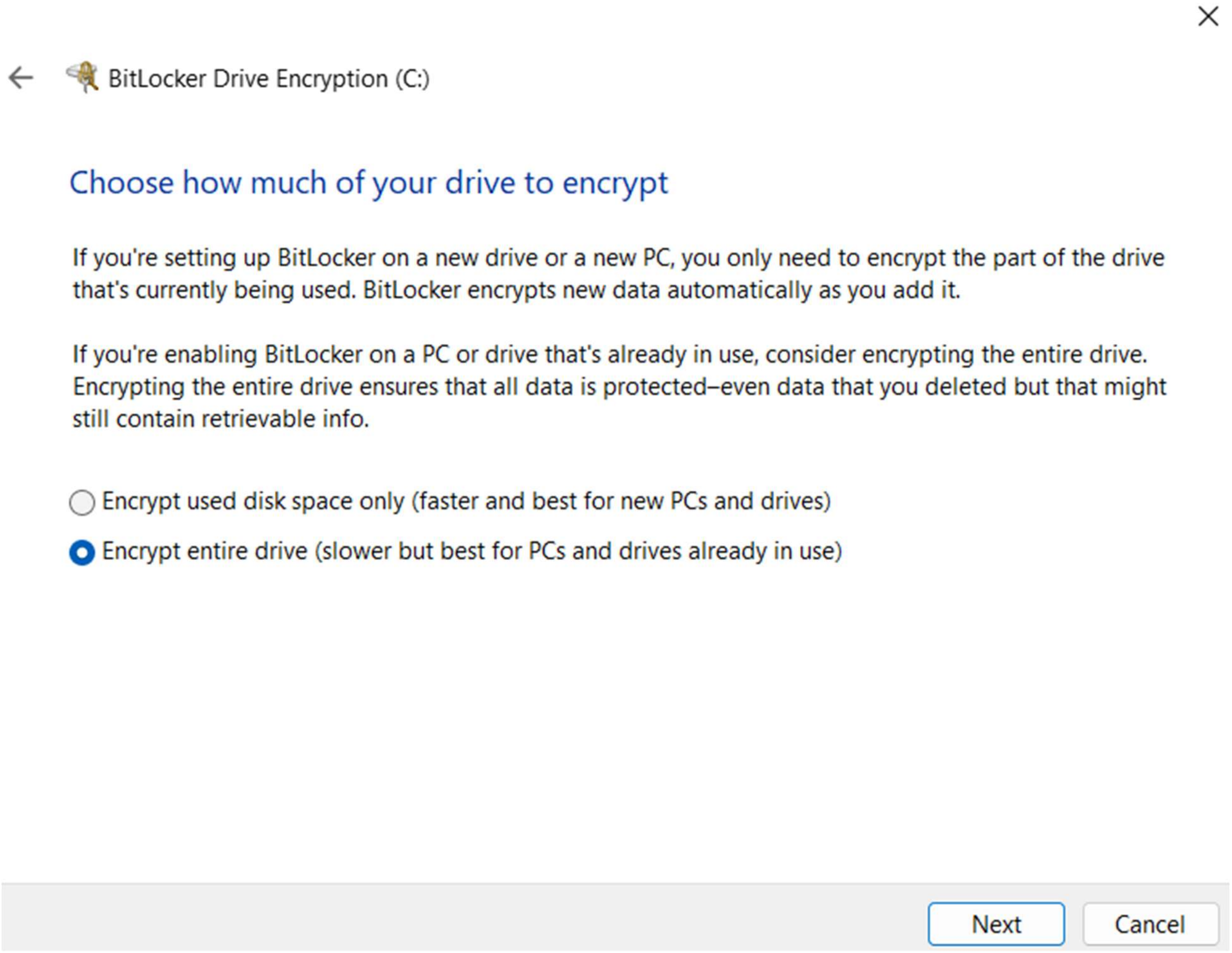
How do you want to back up your recovery key?

Some settings are managed by your system administrator.

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

→ Save to your Microsoft account
→ Save to a file
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel

5. **Here, you can choose whether to encrypt the used disk space or the entire drive (the latter is recommended for security).**



Choose how much of your drive to encrypt

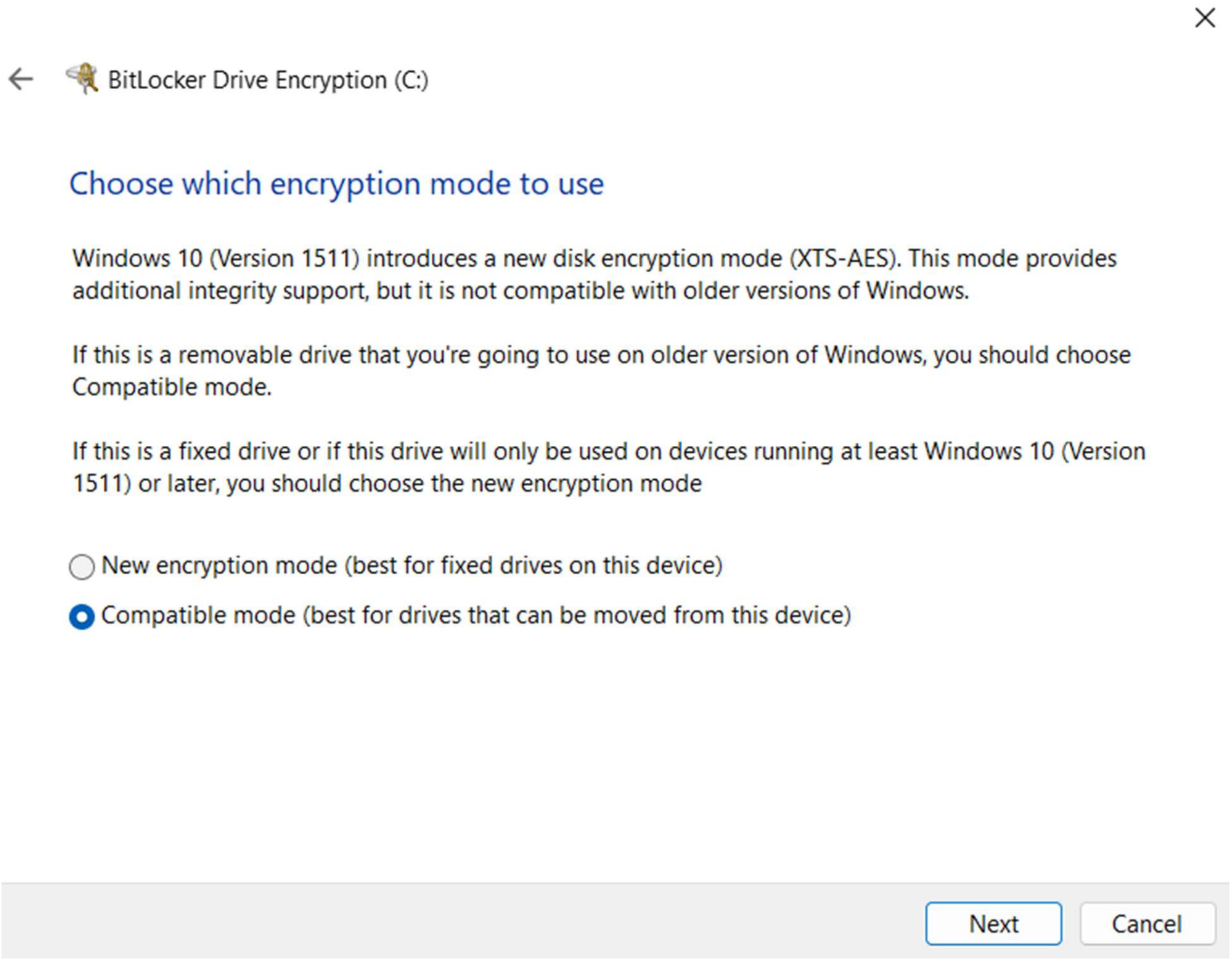
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

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)

6. **After that, you need to choose the compatible mode, as it is recommended.**



BitLocker Drive Encryption (C:)

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.

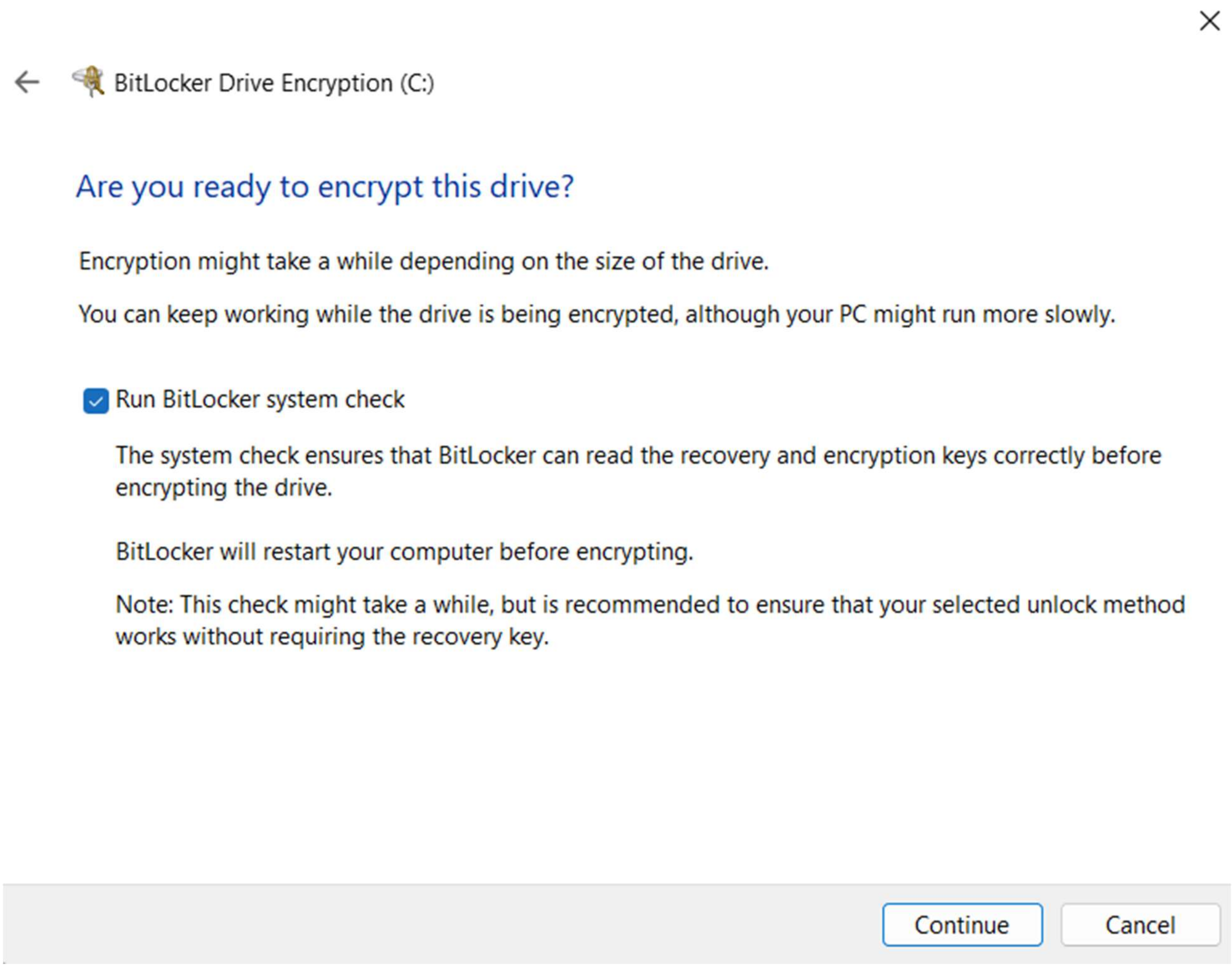
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

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)

7. **Click on Run BitLocker system check**



BitLocker Drive Encryption (C:)

Are you ready to encrypt this drive?

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

You can keep working while the drive is being encrypted, although your PC might run more slowly.

☑ Run BitLocker system check

The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

BitLocker will restart your computer before encrypting.

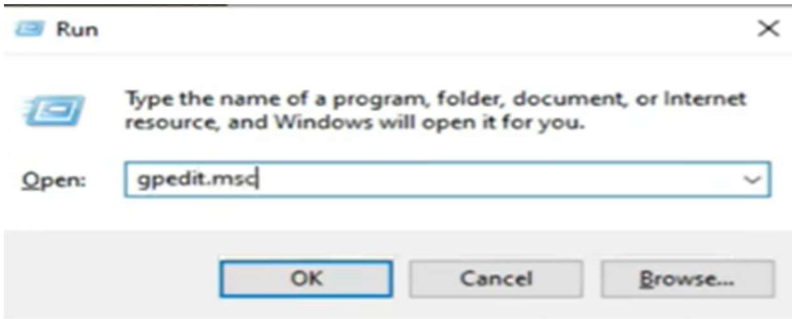
Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.

Scenario 2: BitLocker for Flash Drives

It is almost the same as Scenario 1. You need to set a password for encryption. If TPM 2.0 is not available, BitLocker will still allow you to encrypt the drive, but it will rely on a password or USB key instead of the hardware-based security provided by TPM.

Scenario 3: BitLocker without TPM 2.0

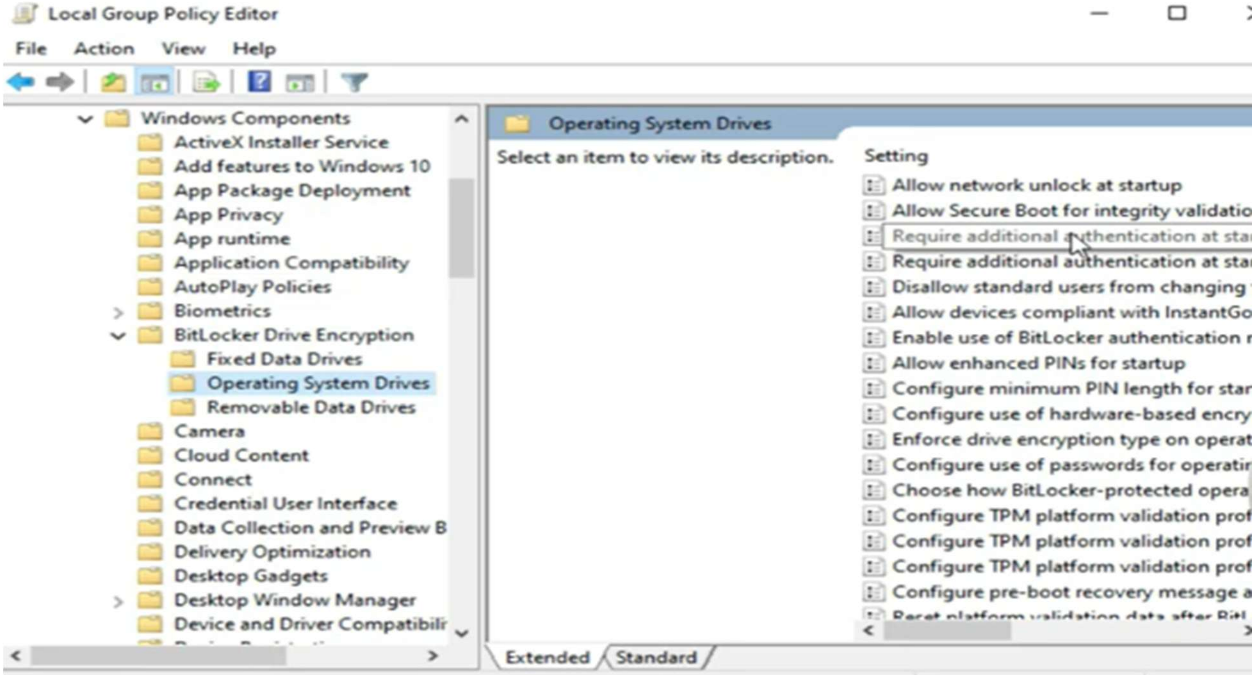
1. **Press Win + R and type gpedit.msc, then press Enter.**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

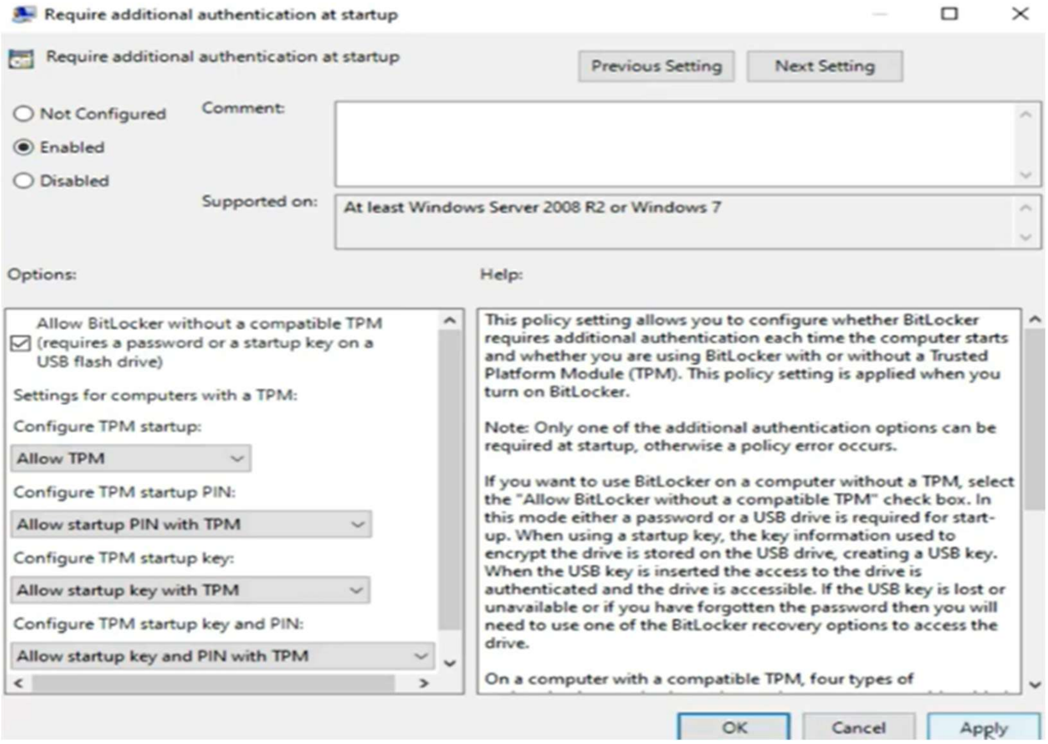
Open: gpedit.msc

2. **Here, go to Administrative Templates → Windows Components → BitLocker Drive Encryption → Operating System Drives → Require additional authentication at startup.**


Local Group Policy Editor
File
Action
View
Help
Windows Components
ActiveX Installer Service
Add features to Windows 10
App Package Deployment
App Privacy
App runtime
Application Compatibility
AutoPlay Policies
Biometrics
BitLocker Drive Encryption
Fixed Data Drives
Operating System Drives
Removable Data Drives
Camera
Cloud Content
Connect
Credential User Interface
Data Collection and Preview B
Delivery Optimization
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibili
Operating System Drives
Setting
Allow network unlock at startup
Allow Secure Boot for integrity validatio
Require additional authentication at sta
Require additional authentication at sta
Disallow standard users from changing
Allow devices compliant with InstantGo
Enable use of BitLocker authentication r
Allow enhanced PINs for startup
Configure minimum PIN length for star
Configure use of hardware-based encry
Enforce drive encryption type on operat
Configure use of passwords for operatin
Choose how BitLocker-protected opera
Configure TPM platform validation prof
Configure TPM platform validation prof
Configure TPM platform validation prof
Configure pre-boot recovery message a
Reset platform validation data after Bitl
Extended
Standard

Select an item to view its description.

3. **Next, click on Enable, then Apply, and OK. The rest of the process is the same as with TPM 2.0.**



Require additional authentication at startup

Require additional authentication at startup

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Server 2008 R2 or Windows 7

Options:

☑ Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup: Allow TPM

Configure TPM startup PIN: Allow startup PIN with TPM

Configure TPM startup key: Allow startup key with TPM

Configure TPM startup key and PIN: Allow startup key and PIN with TPM

Help:

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of

Resources:

https://github.com/alihuseynliofficial/bitlocker-tpm-and-usb-demo

https://youtu.be/Oi6IWjLwv_Q?si=MoPpzg95FcSH4V-i