Overview

If your PC is eligible, you just need to enable BitLocker, choose an unlock method, and set a few other options. Once enabled, files are encrypted as they are added.

Requirements to Use Bitlocker

1 Correct Windows Version
- Win 10 - Education, Professional, or Enterprise
- Win 8 - Professional or Enterprise
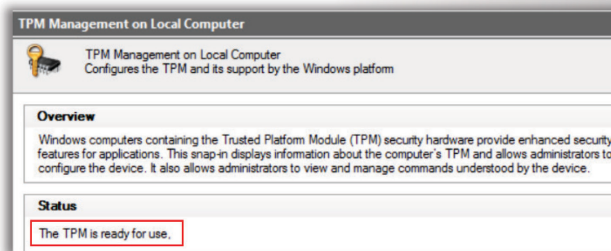- Win 7 - Enterprise or Ultimate

a Check Your Windows Version
1. Go to the **Start** menu.
2. Type *winver* in the search box and a pop-up window will appear with your Windows version.

---

2 Enabled Trusted Platform Module (TPM)

a Check Your TPM Status
1. Go to the **Start** menu.
2. Type *TPM.msc* in the search box. The status should be ready for use.

TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview
Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status
The TPM is ready for use,
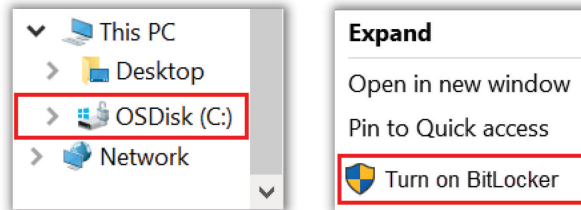
---

3 Administrator access

a Check Your Access

1. Go to the **Start** menu.
2. Type *user accounts* in the search box and then select it.
3. Select **Manage User Accounts**.
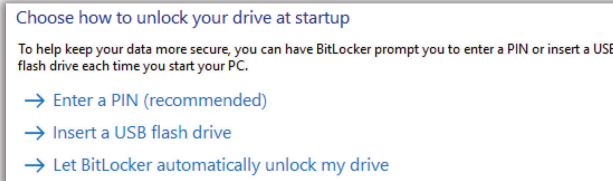4. The access should be Administrator.

Enabling BitLocker

If you meet the requirements in 1, 2, and 3, follow the steps below.
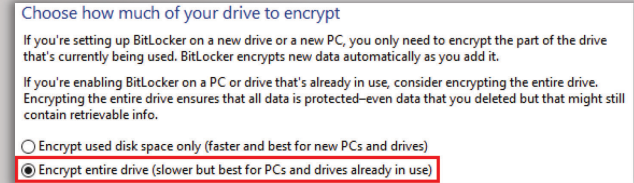
1. Press the Windows button and E (Win + E).
2. Scroll down on the left column.
3. Right-click on the C drive and then select **Turn on BitLocker**.

This PC
> Desktop
> OSDisk (C:)
> Network

Expand
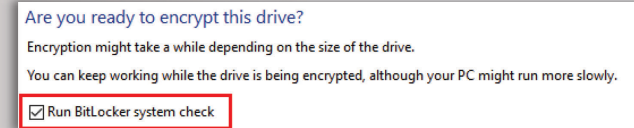Open in new window
Pin to Quick access
Turn on BitLocker

4. After BitLocker scans your PC follow the steps in the pop-up wizard.
5. Choose an Unlock Method then select **Next**.
6. Follow the steps to back up your recovery key then print or save it to your Microsoft OneDrive.

Choose how to unlock your drive at startup

To help keep your data more secure, you can have BitLocker prompt you to enter a PIN or insert a USB flash drive each time you start your PC.

→ Enter a PIN (recommended)
→ Insert a USB flash drive
→ Let BitLocker automatically unlock my drive

---

7. Select **Encrypt entire drive** unless the PC is new. Future files will encrypt with either method.

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)

8. Select **Continue**.
9. Select **Run BitLocker system check** and then select **Continue**.

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

10. To start the encryption process, restart your computer once you are prompted to do so. You can use your computer while your drive is being encrypted.

Lost your unlock method?
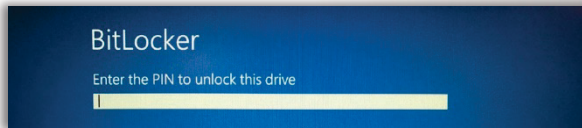- The recovery key will unlock your PC.

Lost your recovery key too?
- Data recovery is not guaranteed.

Logging in

If you chose to automatically unlock your drive on startup then nothing will change for you.

If you chose to enter a PIN or insert a USB flash drive you will need to do so at startup before entering your Windows password.
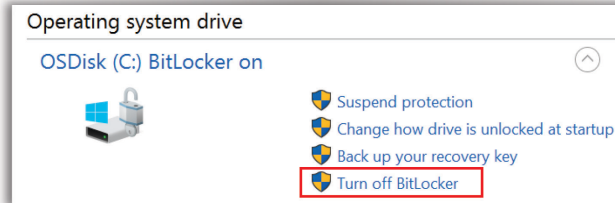

Lost/Forgotten PIN or Flash Drive

Press the escape button on your keyboard when the prompt screen displays. You will then be able to enter your recovery key.

Disabling BitLocker

1. Go to the **Start** menu.
2. Type *Manage Bitlocker* in the search bar and then select it.
3. Select **Turn Off BitLocker**.

4. Select **Turn Off Bitlocker** on the pop-up window to start the decryption process.

Washington University in St. Louis
INFORMATION TECHNOLOGY

Contact the WashU IT Help Desk at 314-933-3333 if you need assistance.

Encrypt your Windows PC with BitLocker

BitLocker, a Microsoft Encryption program that scrambles data so only someone with the right encryption key can unscramble and read it.