

BitLocker is available only on:

- Windows 10 Pro
- Windows 11 Pro
- Enterprise and Education editions

👉 ❌ Not available in:

- Windows Home (you get **Device Encryption** instead, if supported)

To Copilot AI: BitLocker what to do

If BitLocker suddenly asks for a recovery key or you're unsure what to do next, the safest first step is to check where your recovery key is stored and confirm whether BitLocker is actually turned on for your drive. Below is a clear, structured guide based on Microsoft's official documentation.

🔍 1. First: What situation are you in?

Choose the one that matches your case:

A) Windows is asking for a BitLocker recovery key

This happens if:

- Hardware changed (BIOS/UEFI update, TPM reset)
- Windows crashed or updated
- Drive integrity check failed

👉 What to do

- Find your recovery key in one of these places:
 - Your Microsoft account (most common for home users)
 - A printed copy you saved earlier
 - A USB stick where you saved the key
 - Your organization's IT admin (if it's a work laptop)

Microsoft notes that recovery keys can be stored in Microsoft Entra ID / AD DS for managed devices. If you have the 48-digit key, enter it on the blue recovery screen.

B) You want to turn BitLocker ON or OFF

You can manage BitLocker from **Control Panel** → **Manage BitLocker**. Steps from Microsoft Support:

- Sign in with an administrator account
- Open *Manage BitLocker*
- Choose **Turn on BitLocker** or **Turn off BitLocker** for each drive

🔧 2. How to check BitLocker status

You can check via:

Control Panel

- Start → type **BitLocker** → *Manage BitLocker* Shows all drives and their encryption status.

Windows Explorer

- Right-click a drive → *Turn on BitLocker* (if available)

PowerShell (advanced)

Useful for detailed status or scripting.

3. If the drive won't unlock normally

Microsoft provides a **repair tool** (repair-bde.exe) for disaster recovery when a BitLocker drive cannot be unlocked.

This is usually only needed if:

- The drive is corrupted
- Windows cannot boot
- You must connect the drive to another PC as a secondary drive

4. If you don't know where your recovery key is

Here's where to look (in order of likelihood):

1. <https://account.microsoft.com/devices/recoverykey> (**account.microsoft.com in Bing**)
2. A printed page you saved
3. A USB stick labeled "BitLocker Recovery Key"
4. Your work/school IT admin
5. Your Azure AD / AD DS account (for managed devices)

5. Quick decision guide

Situation	What to do
Windows asks for recovery key	Locate key → Enter → Boot normally
You want to disable BitLocker	Control Panel → Manage BitLocker → Turn off
You want to enable BitLocker	Control Panel → Turn on BitLocker → Choose unlock method
Drive won't unlock	Try recovery key → If still failing, use repair tool or another PC
Unsure if BitLocker is on	Check via Control Panel or PowerShell

Want to tell me your exact situation?

If you describe what you see on your screen (e.g., "blue screen asking for key", "Windows won't boot", "I want to turn it off"), I can guide you step-by-step — in Finnish or English, whichever you prefer.

To ChatGPT AI: BitLocker advice

What BitLocker is

BitLocker is full-disk encryption built into **Windows** (Pro, Enterprise, and some Education editions). It protects your data if your computer is lost, stolen, or accessed offline.

When you should use it

Use BitLocker if you:

- Have a **laptop** (highest priority)
 - Store **sensitive or personal data**
 - Travel or work in public places
 - Want protection against someone removing your drive and reading it elsewhere
-

Before turning it on (important)

1. **Back up your data**

Encryption is safe, but mistakes or hardware failure can still cause data loss.

2. **Save your recovery key**

This is critical. If you forget your password or something changes (e.g. motherboard), you'll need it.

- Save to Microsoft account
- Save to USB
- Print it (old-school but reliable)

3. **Check your Windows version**

BitLocker requires Windows Pro or higher. Home uses "Device Encryption" (a simpler version).

Best setup practices

- **Use TPM (Trusted Platform Module)** if available
Most modern PCs have it—this allows automatic unlocking at boot.
 - **Add a PIN (recommended)**
Adds a second layer beyond TPM (good balance of security and usability).
 - **Encrypt the entire drive (not just used space)**
Slower initially, but more secure for older machines.
-

Password & key advice

- Use a **strong password/PIN**, but make it memorable
- Store the recovery key in **at least two places**
- Don't keep the only copy on the same PC

To ChatGPT AI: How to turn on BitLocker

Here's a **simple, safe step-by-step guide** to turn on **BitLocker** in **Windows**:

Turn on BitLocker (easy method)

1. Open BitLocker settings

- Press **Start**
 - Type: **BitLocker**
 - Click **“Manage BitLocker”**
-




2. Choose your drive

You'll see your drives listed (usually **C:** for system)

 Click **“Turn on BitLocker”**

3. Choose how to unlock

You'll be asked how you want to unlock your drive:

-  **TPM only** (automatic – easiest)
-  **PIN** (recommended for extra security)
-  **Password** (less common for system drives)

 Best choice: **TPM + PIN**

4. BACK UP YOUR RECOVERY KEY

This is the most important step.

Choose one or more:

- Save to your Microsoft account
- Save to USB
- Save to a file
- Print it

 **Do NOT skip this**

5. Choose encryption type

- **Used disk space only** → faster (good for new PCs)
 - **Entire drive** → more secure (better for older PCs)
-

6. Choose mode

- **New encryption mode (XTS-AES)** → for modern systems
- **Compatible mode** → if you might move the drive to older PCs

 Usually: **New mode**

7. Start encryption

- Click **Start encrypting**
 - It runs in the background (you can still use your PC)
-

How long does it take?

- SSD: often **minutes to 1–2 hours**
- HDD: can take **several hours**

✔ After it's enabled

- You may be asked for your **PIN at startup**
- Your drive is now protected if the device is lost or stolen

🚨 Important tips

- Keep your **recovery key safe (2 copies recommended)**
- Before BIOS updates → **Suspend BitLocker**
- Don't forget your PIN/password

❓ If you don't see BitLocker

You might be on Windows Home → look for:

- **“Device encryption”** instead (simpler version)

If you want, I can tailor the steps exactly to your computer (e.g., Windows 11, laptop model, whether TPM is enabled).

🚨 Common mistakes to avoid

- ❌ Not saving the recovery key
- ❌ Updating BIOS/firmware without suspending BitLocker
- ❌ Forgetting PIN after enabling it
- ❌ Assuming encryption replaces backups (it doesn't)

🔄 When to suspend BitLocker

Temporarily suspend (not turn off) BitLocker before:

- BIOS/UEFI updates
- Major hardware changes
- Some system repairs

⚡ Performance impact

- Usually **minimal on modern PCs** (especially with SSDs)
- Older machines may see a small slowdown

🧠 Extra tip (often overlooked)

BitLocker protects **data at rest** (when the device is off).

It does **not** protect against:

- Malware
- Phishing
- Someone using your unlocked computer

So still use:

- Antivirus
- Updates
- Good password hygiene

👉 **Bottom line** BitLocker is one of the **most effective and low-effort security upgrades** you can enable on a Windows PC—just make absolutely sure your **recovery key safe and accessible**.