Back up your BitLocker recovery key

Windows 10 · https://cleversupport.ca/docs/windows-10/back-up-your-bitlocker-recovery-key/

BitLocker is the Windows encryption technology that protects your data from unauthorized access by encrypting your drive and requiring one or more factors of authentication before it will unlock it. In normal use BitLocker simply unlocks when you successfully sign into Windows.

However, Windows will require a BitLocker recovery key when it detects a possible unauthorized attempt to access the drive. **It's critical that you have a backup copy of this key. If you lose the key, Microsoft support isn't able to provide it, or recreate it for you.**

In most situations your key is backed up when BitLocker is first turned on, but it's a good idea to do a backup of your own.

Note: Do you need to find your key to unlock a device that is locked? See Finding your BitLocker recovery key in Windows.

How to back up the key

1. Tap the Windows Start button and type BitLocker
2. Select the **Manage BitLocker** Control Panel app from the list of search results
3. In the BitLocker app select **Back up your recovery key**

   [The Manage BitLocker Encryption app with an arrow pointing at the option to back up your BitLocker recovery key.]
4. Select where you want the key backed up
   - **Save to your Microsoft Account** - This will save the key in the Recovery Keys library of your Microsoft Account where you can easily get to it from any computer in the future. **Note:** If you're signed into a computer managed by your work or school this may say **Save to your Azure AD account** instead.

- **Save to a USB flash drive** - If you have a flash drive handy you can save the key to it. If your computer asks for the key in the future just insert that USB drive and follow the onscreen instructions. The key takes only a couple of KB of space so the drive doesn't have to be large. **Important:** Don't store this USB flash drive with the key on it with your computer. If a thief were to get the computer, they could steal the flash drive as well and bypass BitLocker encryption, leaving your data vulnerable.
- **Save to a file** - You can save your recovery key as a plain text file on any device. If you need that file in the future just open it with any text editor like Notepad or Microsoft Word and you'll be able to read the key. You won't be able to save it to the BitLocker encrypted drive, so you may have to save it to a USB drive if you don't have a second, unencrypted, volume on the device.

  We recommend copying or moving that text file to your OneDrive Personal Vault for safe and secure storage that can be readily accessed from any device if you need it.
- **Print the recovery key** - You can simply print the recovery key if you prefer. **Important:** Store that printout somewhere safe and don't keep it with the computer. If a thief were to steal the computer and the printed recovery key they could bypass BitLocker encryption, leaving your data vulnerable.

5. Select **Finish**

You can make as many backups as you want. It's not a bad idea to have more than one, just to be safe.