Windows 11 on "Legacy" Computers

What exactly is LEGACY in this context?
Before Demo.

What is Unified Extensible Firmware Interface (UEFI)?

Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace basic input/output system (BIOS) but is compatible with it. The specification is most often pronounced by naming the letters
U-E-F-I.
https://whatis.techtarget.com/definition/Unified-Extensible-Firmware-Interface-UEFI

What is T.P.M. 2.0?

Note: Since July 28, 2016, all new device models, lines or series (or if you are updating the hardware configuration of a existing model, line or series with a major update, such as CPU, graphic cards) must implement and enable by default TPM 2.0 (details in section 3.7 of the Minimum hardware requirements page). The requirement to enable TPM 2.0 only applies to the manufacturing of new devices.

The TPM is a cryptographic module that enhances computer security and privacy. Protecting data through encryption and decryption, protecting authentication credentials, and proving which software is running on a system are basic functionalities associated with computer security. The TPM helps with all these scenarios and more. **Biometrics like Fingerprint & Facial Recognition.**
Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that helps you with actions such as generating, storing, and limiting the use of cryptographic keys.
https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-tpm
tpm.msc
How Windows Uses T.P.M.

https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm

---

What is Device Encryption?

Windows 11 Windows 10. Windows 11Windows 10. Encryption **helps protect the data on your device so it can only be accessed by people who have authorization**. If device encryption isn't available on your device, you might be able to turn on standard BitLocker encryption instead. Requires Windows Pro.

What is my BitLocker recovery key?

Your BitLocker recovery key is a unique 48-digit numerical password that can be used to unlock your system if BitLocker is otherwise unable to confirm for certain that the attempt to access the system drive is authorized.

How do I print my device level Bitlocker key?

Search for "bitlocker"

Where can I find my BitLocker recovery key?

BitLocker ensured that a recovery key was safely backed up prior to activating protection. There are several places that your recovery key may be, depending on the choice that was made when activating BitLocker:

- **In your Microsoft account:** Sign in to your Microsoft account on another device to find your recovery key. If you have a modern device that supports automatic device encryption, the recovery key will most likely be in your Microsoft account. For more, see Device encryption in Windows.

  Note: If the device was set up or BitLocker protection was activated by another user, the recovery key may be in that user's Microsoft account.
- **On a printout:** You may have printed your recovery key when BitLocker was activated. Look where you keep important papers related to your computer.

Finding your BitLocker recovery key in Windows

https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27-0b89-ea08-f143-056f5ab347d6

https://accounts.microsoft.com/devices

Microsoft technical documentation

The home for Microsoft documentation and learning for developers and technology professionals.
https://docs.microsoft.com/en-us/
