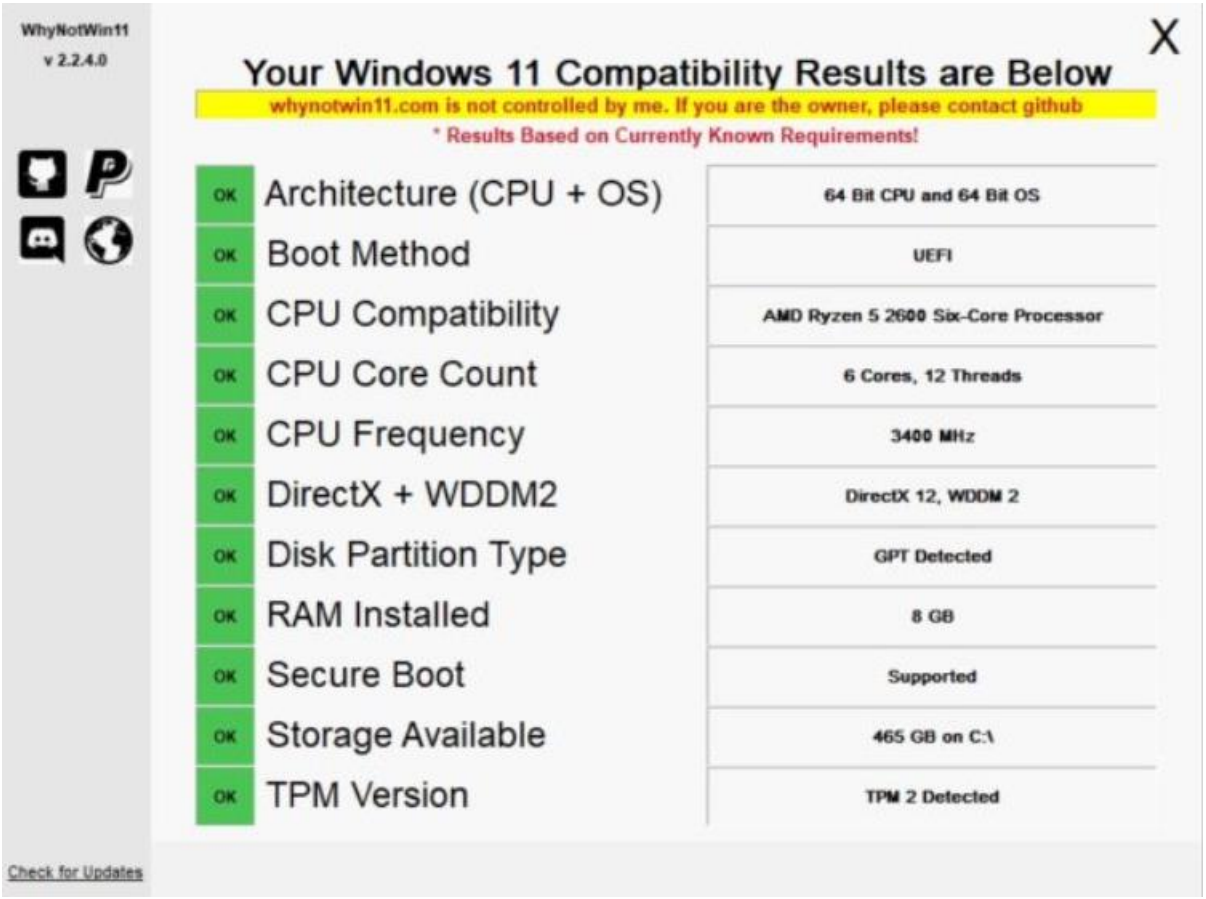
DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung TPM 2.0 nachrüsten oder TPM aktivieren

Stand: 07.02.2022



Der Release von Windows 11 und der mögliche TPM 2.0 – Zwang sorgen dafür, dass einerseits Mainboard-Hersteller ihren Windows 11 und TPM Support betonen und andererseits, dass TPM-Module aufgekauft werden. Wir fassen noch mal die beiden Möglichkeiten zusammen wie man TPM 2.0 auch ohne Modul auf vielen Systemen aktivieren kann und wie man TPM 2.0 nachrüstet. Ein Registry-Eintrag ermöglicht zudem die Systemanforderungen und TPM für Windows 11 Installation gänzlich zu umgehen.

Inhaltsverzeichnis

- Windows 11 ohne TPM und passende Hardware installieren

TPM 2.0 aktivieren im BIOS – so geht's

Bevor man sich in die Online-Shops stürzt und blind irgendwelche Module kauft, sollte man erstmal prüfen, ob TPM 2.0 nicht bereits in der eigenen Hardware integriert ist. Das ist auch bei vielen nicht mehr ganz jungen Systemen der Fall und man kann TPM dort aktivieren. Bei Intel geht das bis zu C232/B250 zurück, bei AMD sieht dies ähnlich aus. Ist eure Hardware aus den letzten 5-6 Jahren, stehen die Chancen gut. Microsoft hat zu dem eine Liste von kompatiblen Intel CPUs und AMD CPUs veröffentlicht. Ärgerlich: AMD Ryzen CPUs der ersten Gen. sind nicht kompatibel.

Sowohl bei AMD als auch Intel müssen **zwei Optionen** für TPM aktiviert werden.

TPM 2.0 aktivieren für Intel-Systeme

Bei Intel heißen die notwendigen Optionen „PPT" (Intel Platform Trust Technology) und „Security Device Support"

1. System starten und ins BIOS gehen (je nach Mainboard Entf, F2 oder F12)
2. In das Untermenü „Security" -> „Trusted Computing" navigieren
3. „Security Device Support" einschalten
4. „TPM-Device" auf „PTT" stellen.
5. Speichern und Neustarten

Die Menüpunkte können sich ja nach Hersteller und Generation unterscheiden. So können die Optionen auch unter „**Miscellaneous**" -> „**Intel Platform Trust Technology (PTT**)" oder „**Advanced" -> „PCH-FW Configuration**" (im ASUS BIOS) direkt zu finden sein.

TPM 2.0 bei AMD-Systemen aktivieren

Bei AMD müssen „fTPM" (Firmware TPM) und „Security Device Support" aktiviert werden

1. System starten und ins BIOS gehen (je nach Mainboard Entf, F2 oder F12)
2. Unterpunkt **„Security"->"Trusted Computing"** wählen und dort „AMD CPU fTPM" oder „Firmware TPM" aktivieren
3. Secure Device Support aktivieren
4. Speichern und Neustarten

Auch hier gibt es Abweichungen zwischen den BIOS/UEFI Versionen der Hersteller (ASUS, MSI, usw.). Im Gigabyte BIOS können sich beide Funktionen auch unter **„Peripherals"** befinden. Die Funktion „Security Device Support" ist unter dem weiteren Unterpunkt „**Trusted Computing**" untergebracht.
Im ASUS BIOS befindet sich TPM unter „**Advanced" -> „CPU Configuration"** oder „**Advanced"** -> „**AMD fTPM configuration**„.

Bei einige Modellen muss möglicherweise „BIOS PSP Support" zusätzlich aktiviert werden, damit TPM erkannt wird.

fTPM aktivieren Gigabyte

Security Device Support

Mittlerweile haben die Mainboard-Hersteller auch selbst Anleitungen zur TPM Aktivierung online gestellt:

- ASRock
- Asus
- Biostar
- EVGA
- Gigabyte
- MSI

TPM Aktivieren per BIOS-Update

Als Alternative zur manuellen TPM Aktivierung im BIOS/UEFI haben die Hersteller begonnen BIOS-Updates für die Kompatibilität mit Windows 11 und ab Werk aktivierten TPM zu veröffentlichen. Den Start macht ASUS und präsentiert bereits eine umfangreiche Liste mit Mainboards, die bereits mit einem Update versorgt wurden oder noch eines erhalten.

Secure Boot aktivieren

Microsoft empfiehlt auch Secure Boot für für Windows 11 zu aktivieren! Sollte dies noch nicht der Fall sein, findet man diese Optionen in der Regel im UEFI Menü „Boot“ (ASUS) oder „BIOS“ (Gigabyte), nach der Deaktivierung von CSM.

Secure Boot funktioniert nicht im CSM-Modus, sondern nur nur im UEFI-Mode, der ebenfalls Voraussetzung für Windows 11 ist. Hier findet ihr mehr zu dem Thema.

TPM nachrüsten

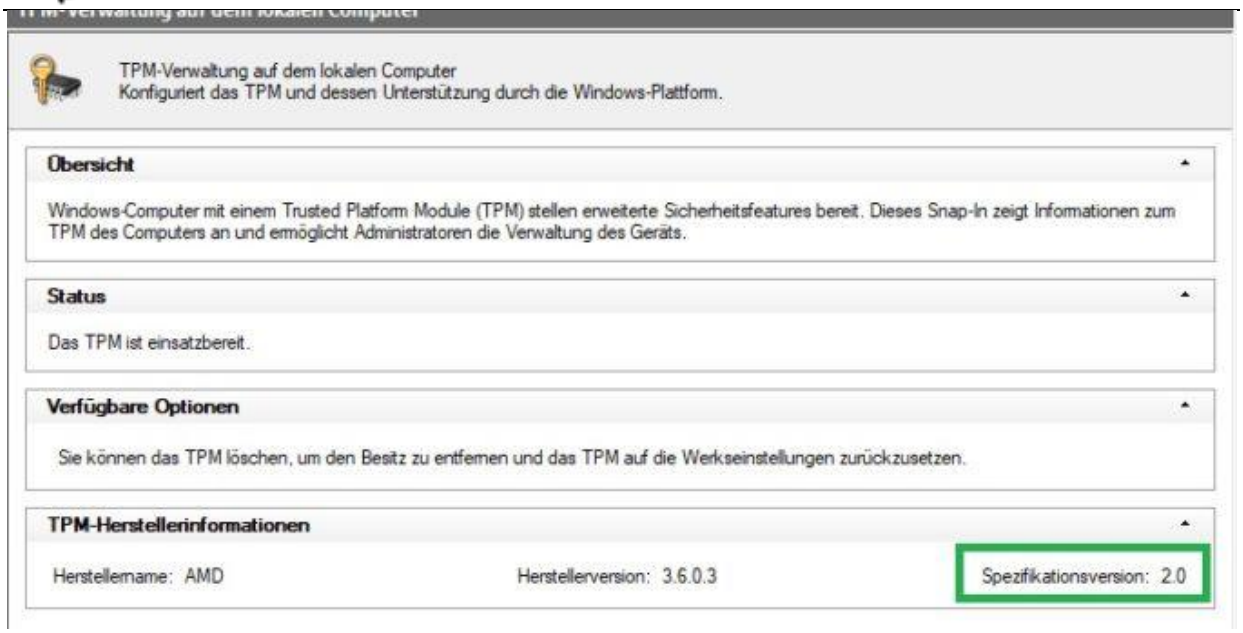
Auch für den Fall, dass man TPM nicht aktivieren kann, gibt es die Möglichkeit TPM 2.0 mit einem Modul nachzurüsten z.B. mit dem ASUS-Modul (13-Pin) (bei amazon)* oder dem ASUS TPM-Modul mit 14+1 (bei amazon)*.
Achtung: Vorrausetzungen dafür ist zum einen ein TPM-Header auf dem Mainboard, also dass ein Anschluss für ein solches Modul vorhanden ist. Außerdem muss das TPM Modul mit dem Mainboard kompatibel sein. Die Hersteller wie ASUS, Gigabyte und ASRock usw. setzen hier unter Umständen auf andere PIN-Layouts, wie man am ASRock TPM-Modul (bei amazon)* sieht

Ein weiterer Nachteil ist, dass diese Module ohnehin nicht immer in großen Stückzahlen in den Online-Shops verfügbar waren und der Hype um Windows 11 die bereits Situation verschärft hat. Die Preise der günstigen Module sind angestiegen und die Lieferbarkeit nur eingeschränkt gegeben.

So testet man ob TPM aktiviert ist

Windows hat bereits Mittel an Bord, mit denen man testen kann, ob TPM aktiviert ist

1. Startmenü öffnen oder Windows-Taste+R drücken
2. „tpm.msc“ eingeben und bestätigen



TPM 2.0 aktiv

In dem Fenster wird angezeigt ob und in welcher Version TPM vorhanden ist.

Windows 11 Systemanforderungen prüfen

Mit den Optionen sollte die Vorrausetzungen für Windows 11 bereits erfüllt werden. Ob auch der Rest des PCs die Anforderungen erfüllt kann mit einem Windows 11 Test Tool wie die dem Microsoft PC Health Check oder WhyNotWin11 schnell überprüft werden.

Windows 11 Systemanforderungen umgehen

Noch ist es möglich die Systemanforderungen auch bezüglich TPM zu umgehen und Windows 11 ohne entsprechende Hardware zu installieren. Die Überprüfung kann dabei sowohl für das Update/Upgrade auf Windows 11 umgangen werden, also auch für die Neuinstallation.

Auch mit der Windows 11 ISO soll eine Installation ohne erfüllte Systemanforderungen möglich sein, allerdings werden dann unter Umständen keine Sicherheitsupdates von Microsoft mehr ausgespielt. Unter dieser Voraussetzung raten wir von einer Installation ab

Achtung: Alle Angaben ohne Gewähr und auf eigene Gefahr!

Windows 11 Upgrade ohne TPM

Die Überprüfung der Systemanforderungen lässt sich bei einem Update auf Windows 11 mit einem einzigen Registry-Eintrag umgehen. Dazu muss man in der Registry und **HKEY_LOCAL_MACHINE\SYSTEM\Setup\MoSetup** einen neuen **DWORD (32-bit)** Eintrag namens „**AllowUpgradesWithUnsupportedTPMOrCPU**“ mit dem **Wert 1** erstellen.

Das kann man manuell oder bequem über eine Datei machen – so geht’s:

1. Texteditor öffnen (Rechtsklick auf den Desktop->Neu->Textdokument)

2. Folgenden Inhalt reinkopieren:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\Setup\MoSetup]
"AllowUpgradesWithUnsupportedTPMOrCPU"=dword:00000001
```

3. Datei als .reg-Datei speichern, also zum Beispiel als „update.reg“.
4. Die erstellte Datei per Doppelklick ausführen
5. System neu starten und das Update starten

Windows 11 ohne TPM und passende Hardware installieren

Auch für die Neu-Installation von Windows 11 lassen sich die derzeit Anforderungen umgehen und zwar nicht nur die an TPM und Secure Boot, sondern auch an RAM-Konfiguration

1. Installation starten bis die Meldung „*Auf diesem PC kann Windows 11 nicht ausgeführt werden*“ erscheint, mit OK bestätigen
2. „Shift + F10“ drücken, um die Eingabeaufforderung zu öffnen
3. „regedit“ eingeben und **HKEY_LOCAL_MACHINE -> SYSTEM** navigieren
4. Dort einen neuen Schlüssel (Key) erstellen mit dem Namen „**LabConfig**„
5. In LabConfig werden per „Rechtsklick“->“Neu“ insgesamt fünf „**DWORD-Werte**“ (32 Bit) mit dem **Wert 1** erstellt. Die Werte heißen: „**BypassTPMCheck**„,“**BypassSecureBootCheck**„,“**BypassRAMCheck**„,“**BypassStorageCheck**“ und „**BypassCPUCheck**„
6. Registrierungseditor schließen und „exit“ in die Eingabeaufforderung eingeben.
7. In der Windows-Installation auf zurück klicken und den Prozess neu beginnen, nun sollte die Installation ohne TPM und Secure Boot funktionieren.

Die Tipps funktionieren derzeit unter Vorbehalt, da Microsoft solche „Hacks“ offenbar blockieren wird. In diesem Fall ist ein kompatibles System notwendig.

Quelle: https://hardware-helden.de/tpm-2-0-nachruesten-oder-kostenlos-im-bios-aktivieren-windows-11/