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

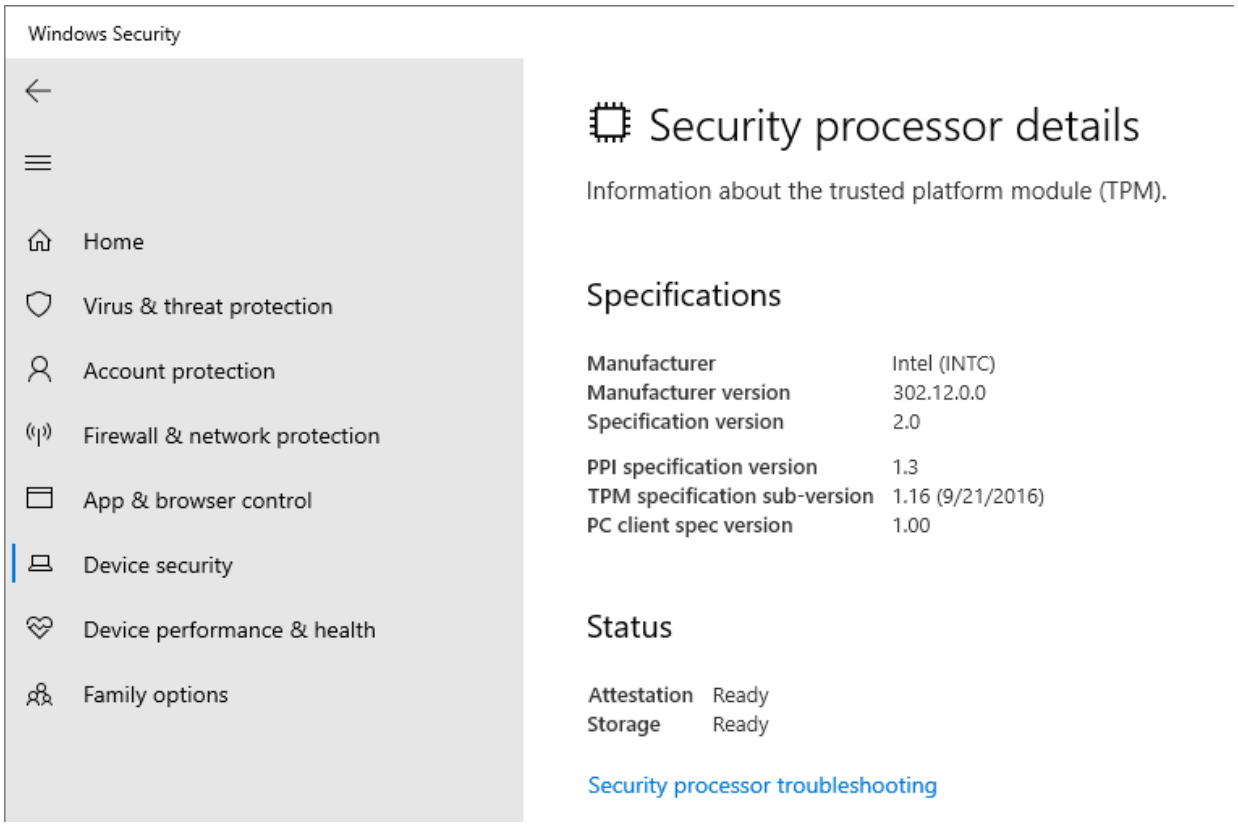
Anleitung TPM überprüfen

Überprüfen Sie den TPM-Status Ihrer Maschine

Es gibt viele verschiedene Möglichkeiten, um zu überprüfen, ob Ihr Computer über ein aktiviertes TPM verfügt.

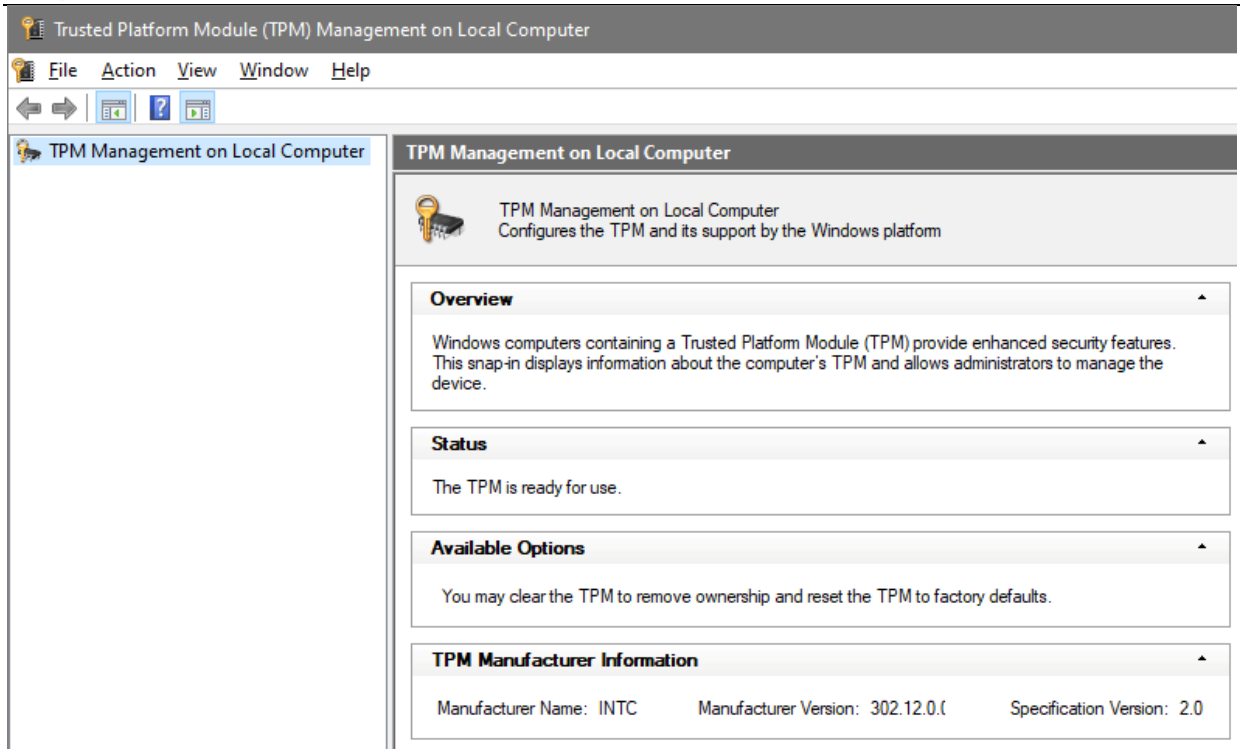
Einstellungen-App

Öffnen Sie die UWP-App „Einstellungen“ auf der Registerkarte „Gerätesicherheit“, indem Sie den URI öffnen `windowsdefender://devicesecurity`. Wenn ein TPM aktiviert ist, sehen Sie einen Link zur Detailseite des **Sicherheitsprozessors** der für ein Intel PTT wie folgt aussieht:

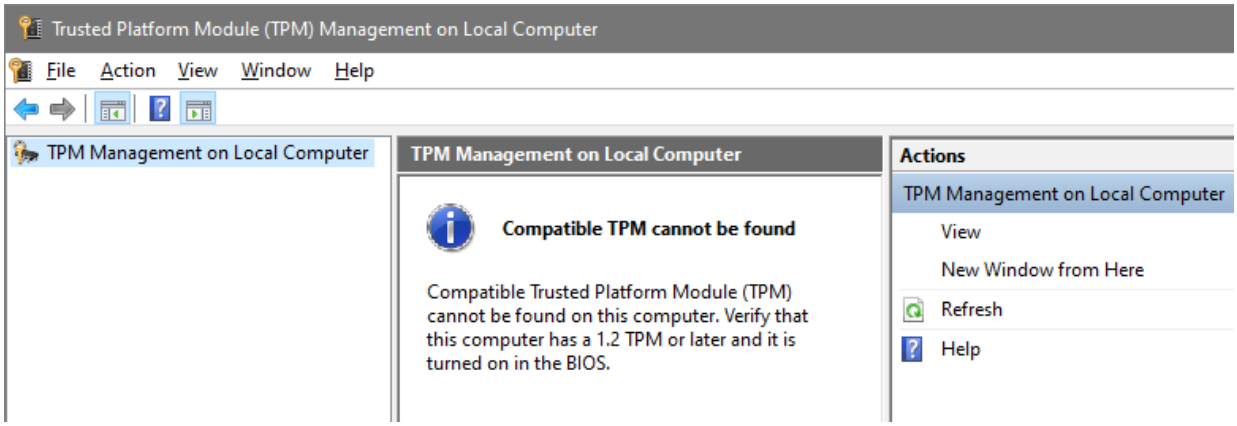


Verwaltungskonsole (MMC)

Open the Windows MMC snap-in `tpm.msc`. If your machine’s TPM is enabled it should look similar to the following:



Wenn das TPM hingegen deaktiviert ist, sieht die MMC so aus:



Befehlszeilentool

Das Windows-Befehlszeilentool tpmtool zeigt detaillierte Statusinformationen an, wenn es mit dem Parameter aufgerufen wird `getdeviceinformation`. Dies erfordert *keine* erhöhten Berechtigungen. Hier ist die Ausgabe einer Maschine mit Intel PTT:

```
C:\>tpmtool.exe getdeviceinformation

-TPM Present: True
-TPM Version: 2.0
-TPM Manufacturer ID: INTC
-TPM Manufacturer Full Name: Intel
-TPM Manufacturer Version: 302.12.0.0
-PPI Version: 1.3
-Is Initialized: True
-Ready For Storage: True
```

```
-Ready For Attestation: True
-Is Capable For Attestation: True
-Clear Needed To Recover: False
-Clear Possible: True
-TPM Has Vulnerable Firmware: False
-PCR7 Binding State: 0
-Maintenance Task Complete: True
-TPM Spec Version: 1.16
-TPM Errata Date: Wednesday, September 21, 2016
-PC Client Version: 1.00
-Is Locked Out: False
```

PowerShell

Das PowerShell-Cmdlet `Get-Tpm`muss mit erhöhten Rechten ausgeführt werden. Seine Ausgabe sieht für eine Intel PTT wie folgt aus:

```
PS C:\> Get-Tpm

TpmPresent                 : True
TpmReady                   : True
TpmEnabled                 : True
TpmActivated               : True
TpmOwned                   : True
RestartPending             : True
ManufacturerId             : 1229870147
ManufacturerIdTxt          : INTC
ManufacturerVersion        : 302.12.0.0
ManufacturerVersionFull20  : 302.12.0.0

ManagedAuthLevel           : Full
OwnerAuth                  : MA9JHWcXmATuXijf7kwOSsCCCxU=
OwnerClearDisabled         : False
AutoProvisioning           : Enabled
LockedOut                  : False
LockoutHealTime            : 10 minutes
LockoutCount               : 0
LockoutMax                 : 31
SelfTest                   : {}
```

Wie Sie oben sehen können, ist die TPM-Version (1.2 oder 2.0) nicht über die verfügbar `Get-Tpm` cmdlet.

WMI

Die WMI-Klasse Win32_Tpm muss mit erhöhten Rechten abgefragt werden. In PowerShell sieht das für eine Intel PTT wie folgt aus:

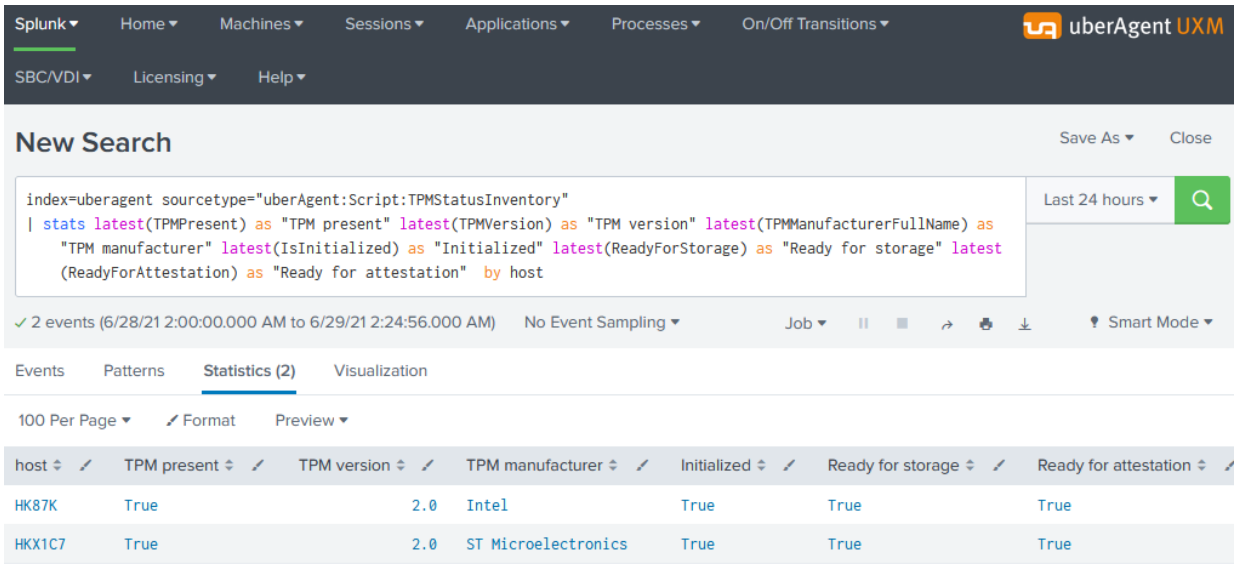
```
PS C:\> Get-WmiObject -Namespace "Root\CIMV2\Security\MicrosoftTpm" -query
"Select * from Win32_Tpm"

__GENUS                    : 2
__CLASS                    : Win32_Tpm
__SUPERCLASS               :
__DYNASTY                  : Win32_Tpm
__RELPATH                  : Win32_Tpm=@
__PROPERTY_COUNT           : 10
```

```
__DERIVATION                 : {}
__SERVER                     : HK87K
__NAMESPACE                  : Root\CIMV2\Security\MicrosoftTpm
__PATH                       :
\\HK87K\Root\CIMV2\Security\MicrosoftTpm:Win32_Tpm=@
IsActivated_InitialValue     : True
IsEnabled_InitialValue       : True
IsOwned_InitialValue         : True
ManufacturerId               : 1229870147
ManufacturerIdTxt            : INTC
ManufacturerVersion          : 302.12.0.0
ManufacturerVersionFull20    : 302.12.0.0
ManufacturerVersionInfo      : Intel
PhysicalPresenceVersionInfo  : 1.3
SpecVersion                  : 2.0, 0, 1.16
PSComputerName               : COMPUTERNAME
```

Bitte beachten Sie das Format der `SpecVersion`Feld: Hauptspezifikationsversion, Nebenspezifikationsversion, Spezifikationsrevision. Wenn Sie nach der TPM-Version suchen, interessiert Sie wahrscheinlich nur die Hauptversion (2.0 oder 1.2).

uberAgent (TPM-Statusinventar)

Als Unternehmen benötigen Sie eine Bestandsaufnahme des TPM-Status Ihrer Geräte. Sie einen Blick auf diesen uberAgent-Praxisleitfaden , der erklärt, wie Sie den regulären TPM-Status von einer beliebigen Anzahl von Endpunkten erfassen. Die Ergebnisse werden zur einfachen Analyse und Berichterstellung in Splunk gespeichert:



Aktivieren Sie fTPM/PTT der CPU

Um das integrierte TPM Ihrer CPU in die UEFI-Einstellungen (früher das BIOS-Setup) zu aktivieren, lokalisieren Sie die Einstellung, die oft einfach genannt wird `fTPM`(AMD-CPUs) bzw `PTT`(Intel-CPUs) und aktivieren Sie es.

Vorbehalte

- Bei einigen Mainboards fehlt möglicherweise diese BIOS-Einstellung, um das TPM der CPU zu aktivieren. In diesem Fall ist Ihre einzige Hoffnung ein BIOS-Update.
- TPM 2.0 wird nur im UEFI-Modus unterstützt, nicht im Legacy-BIOS-Modus. Das Umschalten vom BIOS- in den UEFI-Modus kann das Booten eines installierten Betriebssystems verhindern.

Weitere Informationen zu TPMs

Was ist ein TPM?

Ein TPM kann Zufallszahlen und RSA-Schlüssel berechnen, kurze Daten entschlüsseln und Hashes speichern, die beim Booten des Geräts verwendet werden. Ein TPM umfasst in einer einzigen Komponente:

- Ein RSA-2048-Bit-Schlüsselgenerator
- Ein Zufallsgenerator
- Nichtflüchtiger Speicher zum Speichern von EK-, SRK- und AIK-Schlüsseln
- Eine kryptografische Engine zum Verschlüsseln, Entschlüsseln und Signieren
- Flüchtiger Speicher zum Speichern der PCRs und RSA-Schlüssel

TPM 1.2 vs. TPM 2.0

Der neuere Standard TPM 2.0 bietet Sicherheitsvorteile gegenüber TPM 1.2, das auf die Hash-Algorithmen RSA und SHA-1 beschränkt ist.

TPM 1.2-Teile sind nur als diskrete Siliziumkomponenten (dTPM) verfügbar, während TPM 2.0 auch als Firmware-basierte Komponenten (fTPM) integriert werden kann, z. B. in CPUs.

TPM-Initialisierung

Ab Windows 10 initialisiert das Betriebssystem das TPM automatisch. Dies ist eine Änderung gegenüber früheren Windows-Versionen, bei denen Sie das TPM initialisieren und ein Besitzerkennwort erstellen würden.

Windows-Funktionen, die ein TPM erfordern

Die folgenden Windows-Funktionen erfordern TPM-Unterstützung (Quelle):

Windows feature	TPM version
Gemessener Stiefel	TPM 1.2 oder 2.0
Geräteverschlüsselung	Drehzahl 2.0
Windows Defender-Systemwächter	Drehzahl 2.0
Gesundheitsbescheinigung des Geräts	TPM 1.2 oder 2.0
Virtuelle Smartcard	TPM 1.2 oder 2.0
Autopilot	Drehzahl 2.0
SecureBIO	Drehzahl 2.0
DRTM	Drehzahl 2.0

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

Quelle: https://helgeklein.com/blog/how-to-check-windows-tpm-status-enable-cpu-amd-ftpm-intel-ptt/