



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:

The screenshot shows the Windows Security app interface. On the left, there's a sidebar with icons for Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control, Device security (which is selected), Device performance & health, and Family options. The main pane is titled "Security processor details" and contains the following information:

Specifications

Manufacturer	Intel (INTC)
Manufacturer version	302.12.0.0
Specification version	2.0
PPI specification version	1.3
TPM specification sub-version	1.16 (9/21/2016)
PC client spec version	1.00

Status

Attestation	Ready
Storage	Ready

[Security processor troubleshooting](#)

Verwaltungskonsole (MMC)

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



Trusted Platform Module (TPM) Management on Local Computer

File Action View Window Help

TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview
Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This snap-in displays information about the computer's TPM and allows administrators to manage the device.

Status
The TPM is ready for use.

Available Options
You may clear the TPM to remove ownership and reset the TPM to factory defaults.

TPM Manufacturer Information
Manufacturer Name: INTC Manufacturer Version: 302.12.0.0 Specification Version: 2.0

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

Trusted Platform Module (TPM) Management on Local Computer

File Action View Window Help

TPM Management on Local Computer

Compatible TPM cannot be found

Compatible Trusted Platform Module (TPM) cannot be found on this computer. Verify that this computer has a 1.2 TPM or later and it is turned on in the BIOS.

Actions

TPM Management on Local Computer

- View
- New Window from Here
- Refresh
- Help

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
ManufacturerVersionFull120 : 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 SpecVersionFeld: Hauptspezifikationsversion, Nebenspezifikationsversion, Spezifikationsrevision. Wenn Sie nach der TPM-Version suchen, interessiert Sie wahrscheinlich nur die Hauptversion (2.0 oder 1.2).

überAgent (TPM-Statusinventar)

Als Unternehmen benötigen Sie eine Bestandsaufnahme des TPM-Status Ihrer Geräte. Sie einen Blick auf diesen [überAgent-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:

The screenshot shows the Splunk user interface for the überAgent UX. The top navigation bar includes links for Splunk, Home, Machines, Sessions, Applications, Processes, On/Off Transitions, SBC/VDI, Licensing, and Help. The search bar at the top right contains the query: "index=uberagent sourcetype="uberAgent:Script:TPMstatusInventory" | stats latest(TPMPresent) as "TPM present" latest(TPMVersion) as "TPM version" latest(TPMManufacturerFullName) as "TPM manufacturer" latest(IsInitialized) as "Initialized" latest(ReadyForStorage) as "Ready for storage" latest(ReadyForAttestation) as "Ready for attestation" by host". Below the search bar, it says "Last 24 hours" and has a search icon. The results section shows "2 events (6/28/21 21:00:00.000 AM to 6/29/21 2:24:56.000 AM)" and "No Event Sampling". The "Statistics (2)" tab is selected, showing two rows of data:

host	TPM present	TPM version	TPM manufacturer	Initialized	Ready for storage	Ready for attestation
HK87K	True	2.0	Intel	True	True	True
HKX1C7	True	2.0	ST Microelectronics	True	True	True

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 WALKER - PC-BLITZHELFER - NOTDIENST
Nationalgasse 14 • 72124 Pliezhausen • Tel. 07127 / 890 729 - Fax 89118
Internet: <http://www.pc-blitzhelper.de> – Mobil 0172-882 79 55

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