

Secure Boot



Secure Boot

Was ist Secure Boot ? (sicherer Start)

Der sichere Start ist eine Funktion in UEFI (Unified Extensible Firmware Interface), mit dem sichergestellt wird, dass während der Startsequenz eines Geräts nur vertrauenswürdige Software ausgeführt wird. Dabei wird die digitale Signatur der Pre-Boot-Software anhand einer Reihe vertrauenswürdiger digitaler Zertifikate überprüft, die in der Firmware des Geräts gespeichert sind. Als Branchenstandard definiert UEFI Secure Boot, wie die Plattformfirmware die Zertifikate verwaltet, die Firmware authentifiziert und wie das Betriebssystem (OS) mit diesem Prozess verbunden ist.

Secure Boot

Microsoft aktualisiert die ursprünglich 2011 ausgestellten Secure Boot-Zertifikate, um sicherzustellen, dass Windows-Geräte weiterhin vertrauenswürdige Startsoftware überprüfen. Diese älteren Zertifikate liefen seit Juni 2026 ab. Geräte, die die neueren 2023-Zertifikate nicht erhalten haben, werden weiterhin normal gestartet und betrieben, und Standard-Windows-Updates werden weiterhin installiert. Diese Geräte können jedoch keine neuen Sicherheitsmechanismen für den frühen Startprozess mehr erhalten, einschließlich Updates für den Windows-Start-Manager, Datenbanken für den sicheren Start, Sperrlisten oder Risikominderungen für neu entdeckte Sicherheitsrisiken auf Startebene.

Secure Boot

Secure-Boot-Zertifikate:

Auf manchen PCs kann die Aktualisierung der Secure-Boot-Zertifikate wegen älterer oder fehlerhafter UEFI-/BIOS-Firmware nicht korrekt durchgeführt werden. Der PC läuft normalerweise trotzdem weiter und erhält andere Windows-Updates. Langfristig sollte aber ein BIOS-/UEFI-Update des Mainboard- oder PC-Herstellers geprüft werden.

- **BIOS = Basic Input/Output System**

- Grundlegendes Ein-/Ausgabesystem.

- Es ist die ältere Firmware eines PCs und startet beim Einschalten die Hardware und anschließend das Betriebssystem.

- **UEFI = Unified Extensible Firmware Interface**

- Einheitliche erweiterbare Firmware-Schnittstelle.

- Es ist der **moderne Nachfolger des BIOS** und bietet unter anderem schnelleren Start, Unterstützung für große Festplatten und **Secure Boot**.

Secure Boot

Sie können den Status von Secure Boot ganz einfach unter Windows überprüfen.

Methode 1:

1. Drücken Sie **Windows + R**.
2. Geben Sie **msinfo32** ein und drücken Sie **Enter**.
3. Im Fenster **Systeminformationen** suchen Sie nach den Einträgen:
 1. **BIOS-Modus**
 1. Sollte **UEFI** lauten.
 2. **Sicherer Startzustand** (Secure Boot State)
 1. **Ein** = Secure Boot ist aktiviert.
 2. **Aus** = Secure Boot ist deaktiviert.
 3. **Nicht unterstützt** = Der PC ist im Legacy-Modus gestartet oder unterstützt Secure Boot nicht.

Secure Boot

Methode 2: Windows-Sicherheit

1. Öffnen Sie **Einstellungen** → **Datenschutz und Sicherheit** → **Windows-Sicherheit**.
2. Klicken Sie auf **Gerätesicherheit**.
3. Unter **Sicherer Start** sehen Sie, ob Secure Boot aktiviert ist.

Wenn Secure Boot deaktiviert ist

Damit Secure Boot aktiviert werden kann, müssen folgende Voraussetzungen erfüllt sein:

- ✓ BIOS-Modus: **UEFI**
- ✓ Datenträger: **GPT** (nicht MBR)
- ✓ Legacy-Modus im BIOS deaktiviert
- ✓ Secure Boot eingeschaltet

Secure Boot

Grundsätzlich gilt:

- **Für eine offizielle Neuinstallation von Windows 11** gehört Secure Boot zu den empfohlenen bzw. unterstützten Sicherheitsfunktionen.
- **Ein bereits installiertes Windows 11 Home läuft häufig auch mit deaktiviertem Secure Boot**, sofern die Installation bereits erfolgt ist oder Windows auf einem nicht vollständig unterstützten PC installiert wurde.

Vorteile von aktiviertem Secure Boot

- Höherer Schutz vor Schadsoftware beim Systemstart.
- Bessere Zusammenarbeit mit anderen Sicherheitsfunktionen wie:
 - TPM 2.0
 - Windows Defender
 - BitLocker (falls verwendet)
 - Kernel-Schutz und Virtualization-based Security (VBS)

Secure Boot

Wann kann man Secure Boot deaktivieren?

Es gibt einige Ausnahmen, z. B. wenn Sie:

- Linux-Distributionen verwenden, die Secure Boot nicht unterstützen,
- ältere Betriebssysteme starten möchten,
- bestimmte Hardware oder Treiber einsetzen, die nicht signiert sind.

Für einen normalen Windows-11-PC ist das aber eher selten nötig.