

# USB Geräte unter Vista verwalten und Sperren

Beigesteuert von Frank Solinske

## USB Geräte unter Vista verwalten und Sperren

USB Geräte, insbesondere USB Sticks, erfreuen sich besonderer Beliebtheit. Diese Situation ist besonders in Firmennetzwerken eine nicht zu vernachlässigende Sicherheitslücke. Standardmäßig ist für Autostart für Wechseldatenträger eingestellt, was den Befall von Viren und anderer Schadsoftware erleichtert. Durch Windows Vista hat Microsoft an dieser Stelle eine Möglichkeit geschaffen, um die Bedrohungen zu verringern.

Die gezeigte Methode funktioniert nur mit MS Vista und Longhorn Server.

In der GPO gibt es neue Möglichkeiten mit denen man den Zugriff auf USB Geräte steuern kann. Für diesen Artikel nutze ich 2 unterschiedliche USB Sticks, um beide Funktionen zu erläutern.

Modell1 (oben): 128MB JetFlash USB 2.0

Modell2 (unten): 1GB MS USB 2.0

Alle Geräte werden über ihre Hardware ID eindeutig identifiziert. Mit der Hardware ID ist es auch möglich den Zugriff zu steuern. Dazu muss die Hardware ID aus dem Gerätemanager ausgelesen werden. Über Start &ndash; Suche kann man den Gerätemanager direkt aufrufen, indem man devmgmt.msc eingibt und mit Enter bestätigt. Der Warnhinweis der UAC sollte man mit Fortsetzen bestätigen. Zuerst muss man die Eigenschaften des USB Stick aufrufen und dann zur Registerkarte Details wechseln. Hier kann man aus dem Dropdown Feld den Menüpunkt Hardware-IDs auswählen. Für die GPO ist die erste Zeile entscheiden. Diese sollte man sich per Copy & Paste in eine \*.txt Datei exportieren.

Dadurch ergeben sich folgende Hardware-IDs:

Hardware ID: 1 GB Stick: USBSTOR\DiskChipsBnkFlash\_Disk\_\_\_\_\_2.00

Hardware ID 128 MB Stick: USBSTOR\DiskJetFlashTS128MJF2A\_\_\_\_\_1.00

Damit die GPO greift, darf der USB Stick nicht am System angeschlossen gewesen sein. Ist dieses der Fall dann muss man den Stick deinstallieren. Dazu wählt man im Gerätemanager den USB Stick aus und ruft mit einem Rechtsklick den Punkt Deinstallation aus dem Kontextmenü auf.

Den Gerätemanager erreicht man über:

Start &ndash; Systemsteuerung &ndash; System und Wartung &ndash; Geräte Manager

Die Sperrung der USB Wechselmedien wird nun in der GPO eingetragen. Über Start &ndash; Suchen startet man den Gruppenrichtlinieneditor mit dem MMC Befehl: gpedit.msc

Den UAC Warnhinweis mit Fortsetzen bestätigen, damit die Konsole gestartet wird.

Die entsprechende GPO findet man unter:

Computerkonfiguration &ndash; Administrative Vorlagen &ndash; System &ndash; Geräteinstallation &ndash; Einschränkungen bei der Geräteinstallation

Wenn man komplett die Installation von USB Geräten sperren möchte, dann aktiviert man den folgenden Punkt.

Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind.

Diesen setzt man nun auch aktiviert. Damit man mit einem administrativen Account dennoch USB Sticks nutzen kann, muss man folgende Punkte aktivieren.

Administratoren das Außerkraftsetzen der Richtlinie unter &bdquo;Einschränkungen bei der Geräteinstallation&ldquo;

erlauben.

Somit kann ein Administrator jeden USB Stick nutzen. Will man das noch weiter einschränken, dann kann man gezielt nur einen (oder mehrere USB Sticks) definieren. Die folgende Einstellung muss aktiviert werden. Danach muss die entsprechende Geräte-ID in die Liste eingetragen werden. Installation von Geräten mit dieser Geräte-ID zulassen.

Mit dem Knopf &bdquo;Anzeigen&ldquo; ruft man die Liste auf, in die die entsprechenden Geräte-Id's eingetragen werden.

Über &bdquo;Hinzufügen&ldquo; kann man nun die ID eintragen und mit OK übernehmen.

Das erste Fenster auch mit OK schließen.

Abschließend muss man die Richtlinie übernehmen, indem man entweder das System neu startet, oder über die Command Shell den Befehl &bdquo;gpupdate&ldquo; ausführt.

Namenserklärung:

USB = Universal Serial Bus  
MS = Microsoft  
GPO = Group Policy Object  
UAC = User Account Control  
MSC = Management Saved Console  
MMC = Microsoft Management Console

© 2007 by Frank Solinske &ndash; MVP Windows Server Security