ZUGRIFF AUF WECHSELDATENTRÄGER VERHINDERN

Viele SchülerInnen arbeiten auch in der Schule immer öfters mit USB-Sticks. Der Markt an portablen Programmen, die direkt vom USB stick gestartet werden, wächst täglich. Programm Suiten, wie die digitale Schultasche erfreuen sich großer Beliebtheit.

Gefordert sind wieder einmal die Administratoren, die nun dafür sorgen müssen, dass nur die „guten“ Programme ins Netz gelangen und die „bösen“ draußen bleiben.

Aber wie verhindert man nun, dass keine „bösen“ Programme (z.B. Sniffer, Keylogger, …) von USB-Sticks gestartet werden, denn portable Programme brauchen keine administrativen Rechte. Und Viren, Trojaner und Würmer werden am häufigsten über USB-Sticks ins Netz eingeschleust. Man denke nur an den Conficker/Downad Wurm, der große Firmen betroffen hat.

DIE HIER VORGESCHLAGENE LÖSUNG GEHT FOLGENDEN WEG:

- Ausführen von Programmen von USB Wechseldatenträgern wird verboten
- Der Schreib-/Lesezugriff auf Dateien wird erlaubt.

VORAUSSETZUNGEN:

- Windows Domäne (2003, 2008)
- USB Drive Letter Manager von Uwe Sieber
- Windows XP, Vista, Windows7

INSTALLATION USB DRIVELETTER MANGAGER (USBDLM)

Auf das Tool wurde in einem früheren Artikel schon hingewiesen.

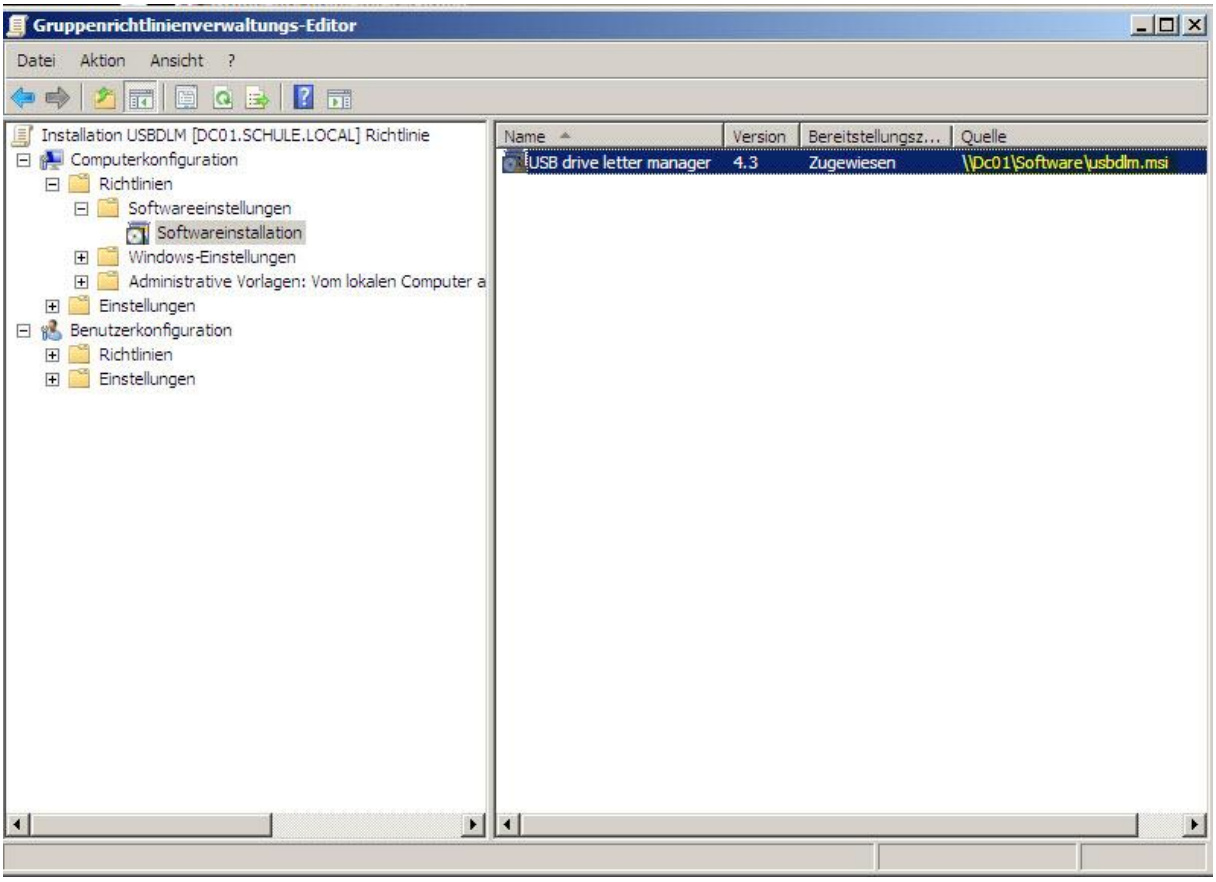
Zum Programm Download

In einem Netzwerk wird das Programm am besten über die Softwareverteilung per Gruppenrichtlinie installiert. (MSI Datei!)

GRUPPENRICHTLINIE ERSTELLEN

COMPUTERKONFIGURATION/RICHTLINIEN/SOFTWAREEINSTELLUNGEN

Achtung: Quelle als UNC Pfad!!



Der Autor der Software USBDLM bietet auch die Möglichkeit an, die angepasste ini Datei in die MSI Datei zu integrieren.

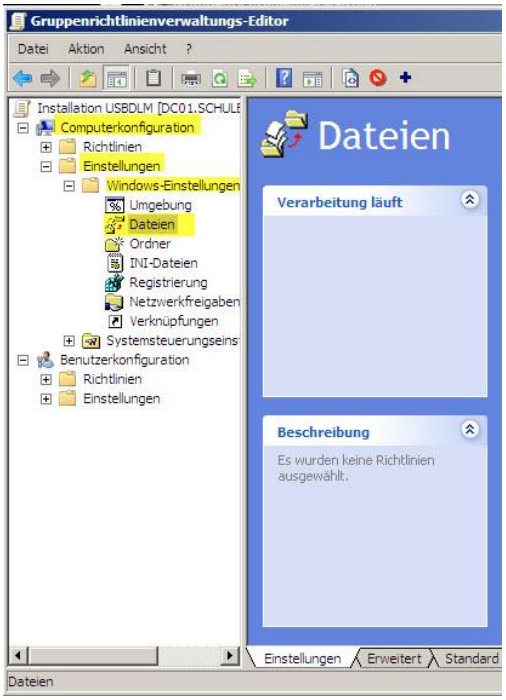
Wir wählen hier aber einen anderen Weg, weil ich auch zeigen möchte, wie perfekt die neuen GPP Group Policy Preferences arbeiten.

Achtung:

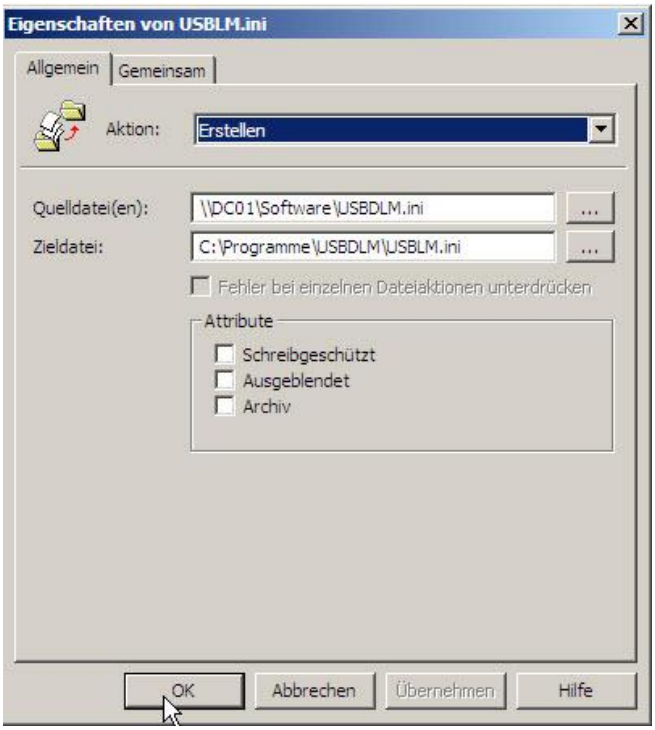
Damit auf den Clients die Preferences greifen müssen die Client Side Extension installiert sein. (KB 943729)

Dazu gibt es auch einen Artikel.

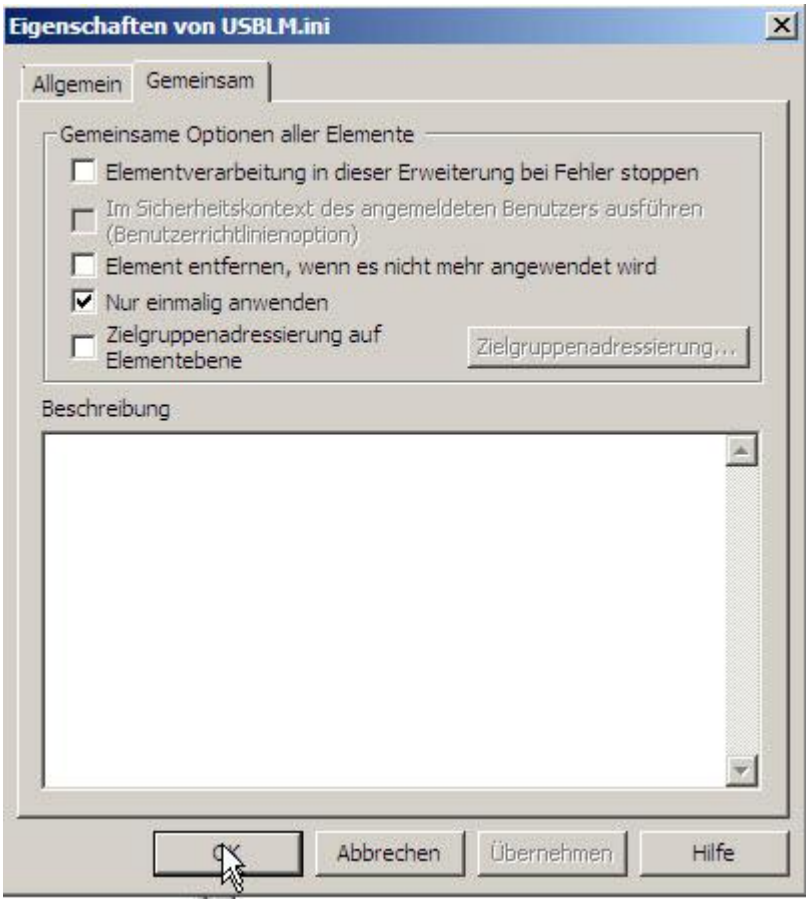
- Wir wählen COMPUTERKONFIGURATION/EINSTELLUNGEN/WINDOWS-EINSTELLUNGEN/DATEIEN



- Rechte Maustaste auf DATEIEN, Aktion ERSTELLEN
- Quelldatei auswählen
- Zieldatei angeben

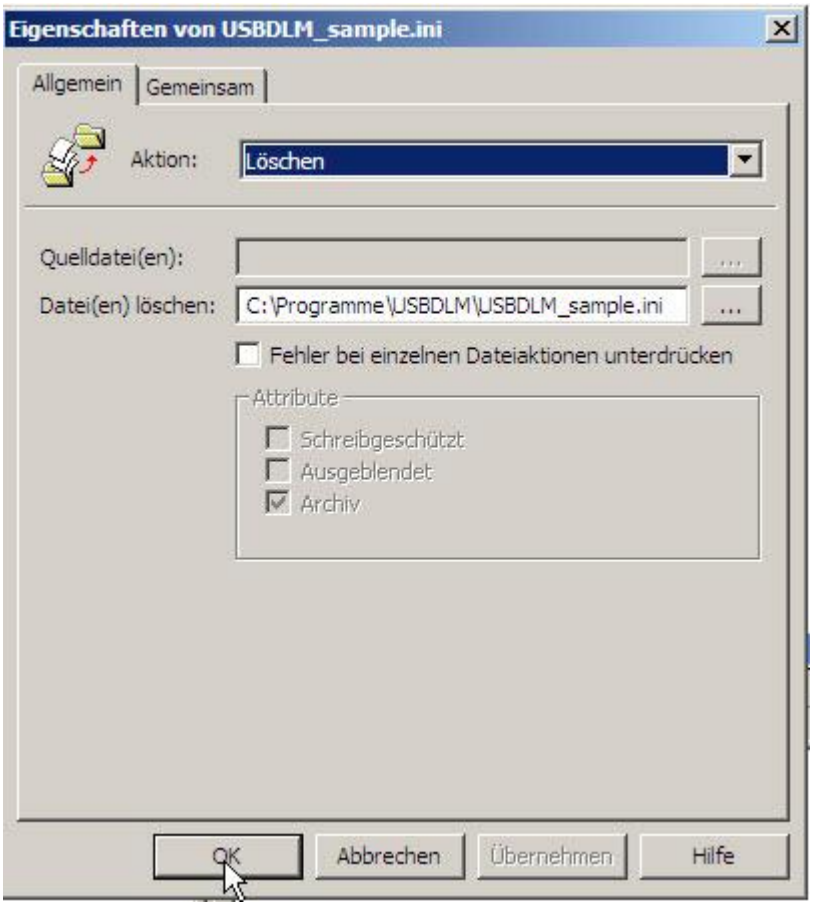


- Karteireiter GEMEINSAM
- Haken bei NUR EINMALIG ANWENDEN

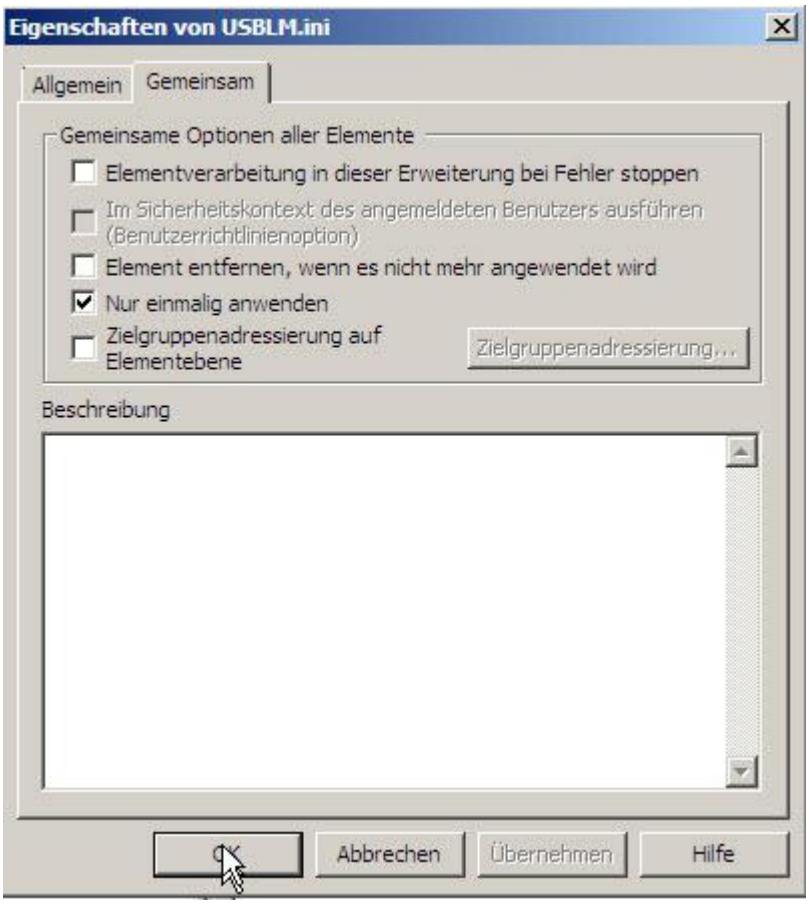


Damit die angepasste INI Datei funktioniert, muss die USBDLM_sample.INI Datei gelöscht werden

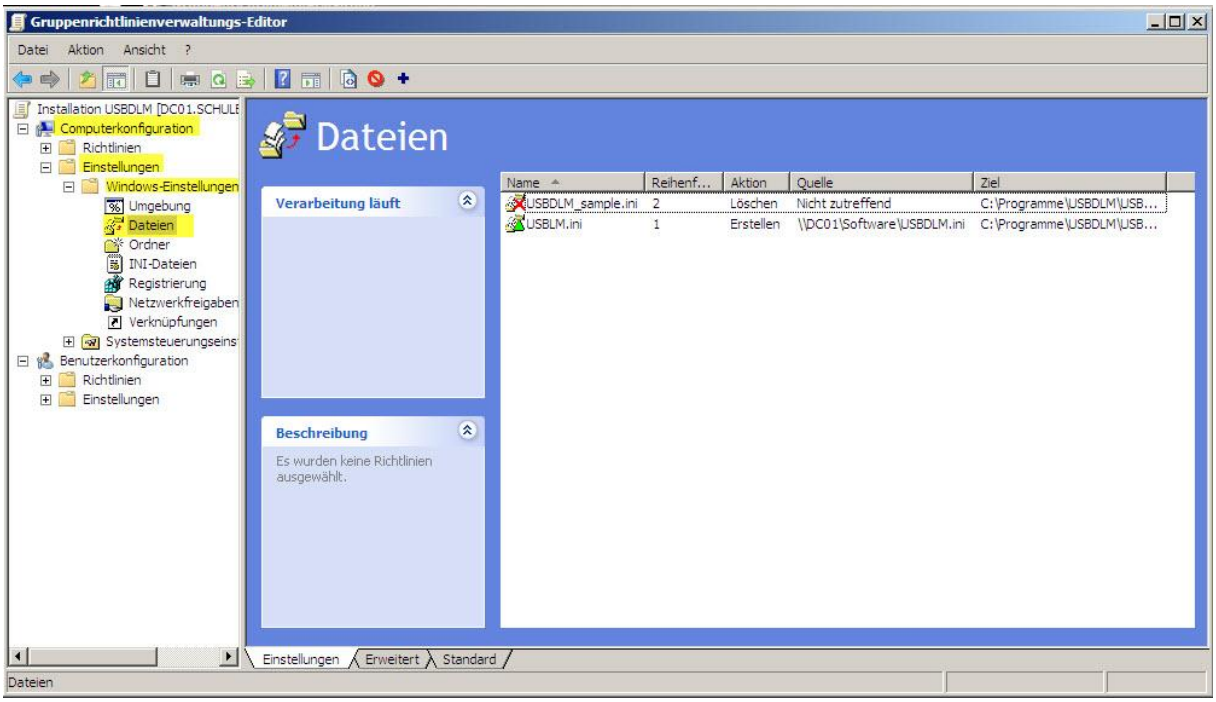
- Rechte Maustaste auf DATEIEN, Aktion LÖSCHEN
- Datei angeben



- Karteireiter GEMEINSAM
- Haken bei NUR EINMALIG ANWENDEN



So sieht die fertige Richtlinie aus:



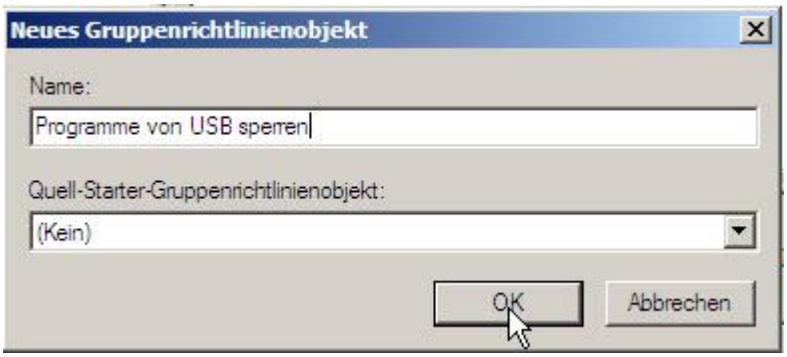
AUSFÜHREN VON PROGRAMMEN VERHINDERN

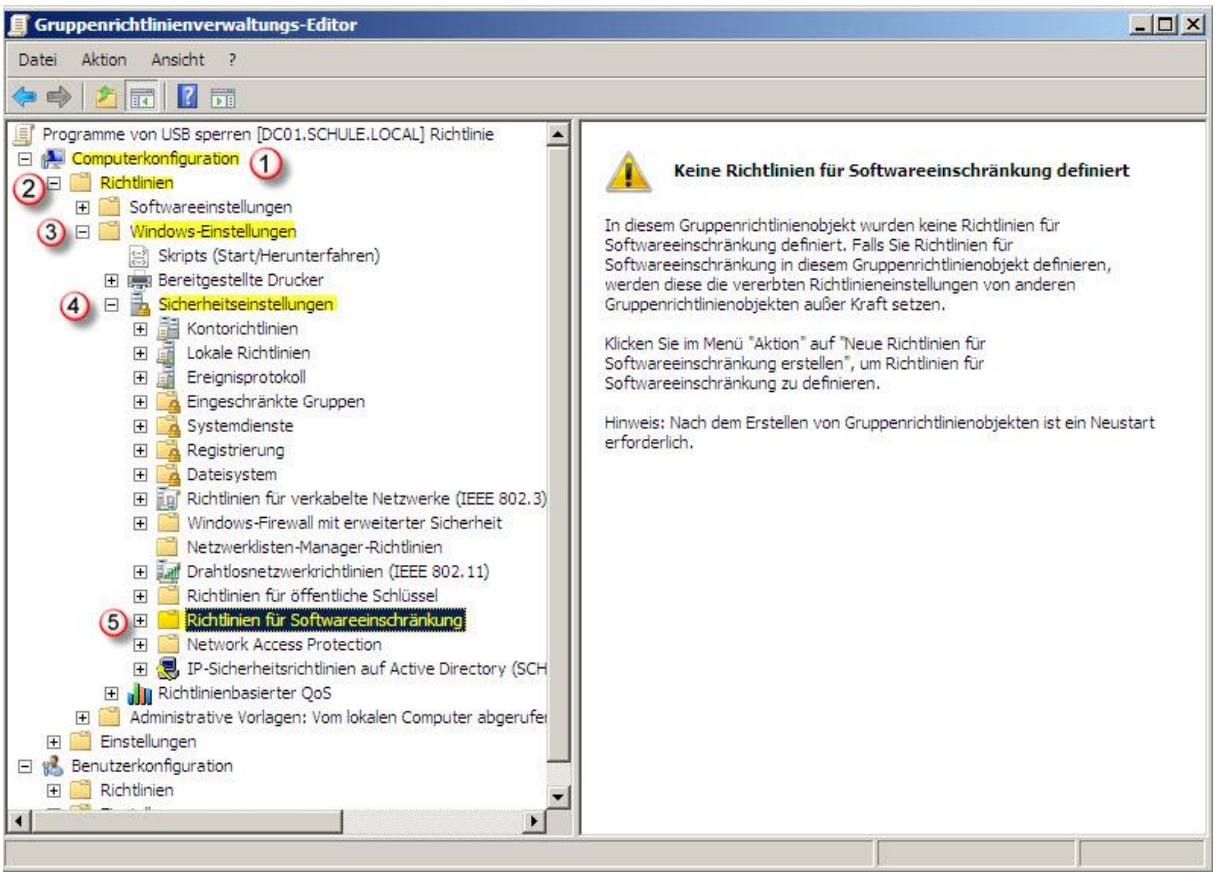
Auch diese Aufgabe lösen wir über eine Gruppenrichtlinie.

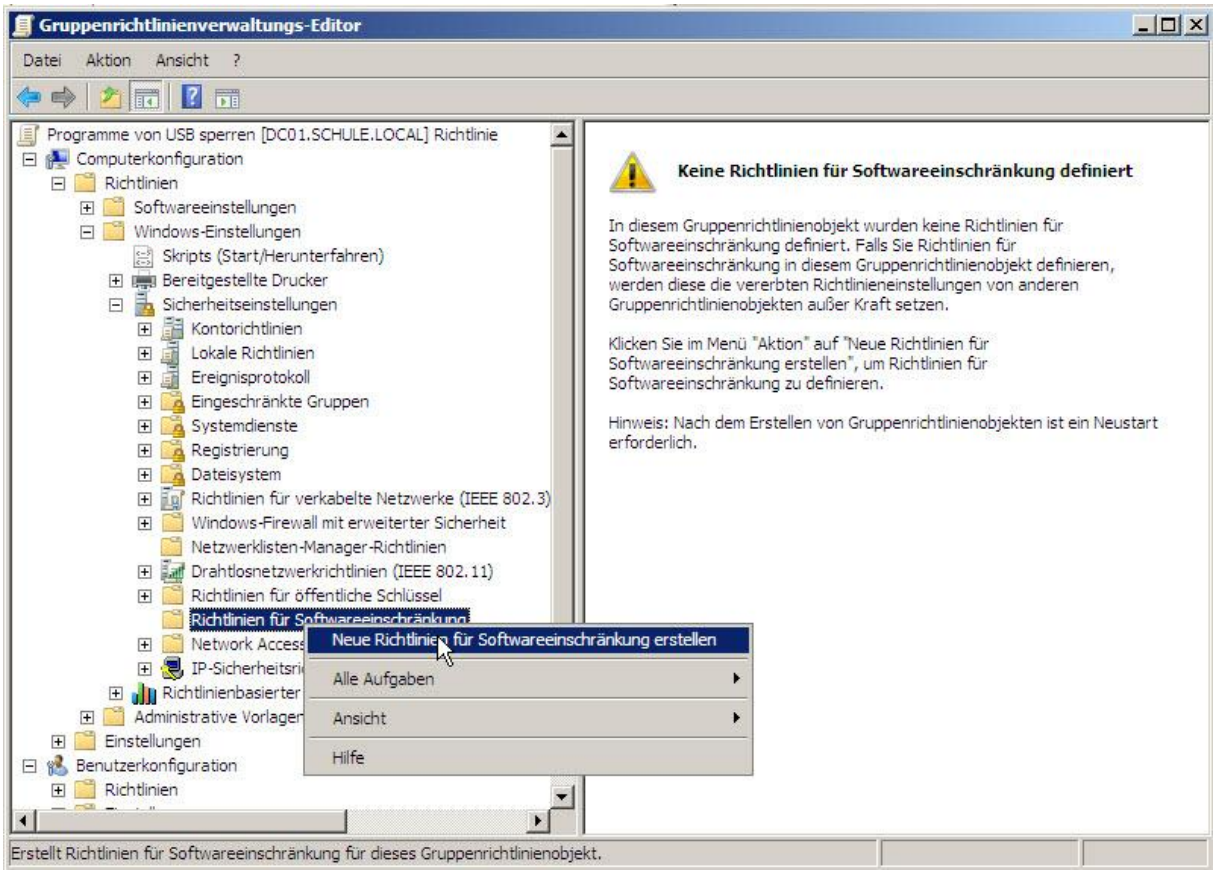
Für die Client Systeme Vista und Windows 7 gibt es in Verbindung mit Windows Server 2008 bzw. Server 2008 R2 neue Gruppenrichtlinien, die den Zugriff auf Wechseldatenträger steuern.

Der hier beschriebene Weg funktioniert aber auch für Windows XP

GRUPPENRICHTLINIE ESRTELLEN




Gruppenrichtlinienverwaltungs-Editor
Datei Aktion Ansicht ?
Programme von USB sperren [DC01.SCHULE.LOCAL] Richtlinie
Computerkonfiguration
Richtlinien
Softwareeinstellungen
Windows-Einstellungen
Skripts (Start/Herunterfahren)
Bereitgestellte Drucker
Sicherheitseinstellungen
Kontorichtlinien
Lokale Richtlinien
Ereignisprotokoll
Eingeschränkte Gruppen
Systemdienste
Registrierung
Dateisystem
Richtlinien für verkabelte Netzwerke (IEEE 802.3)
Windows-Firewall mit erweiterter Sicherheit
Netzwerklisten-Manager-Richtlinien
Drahtlosnetzwerkrichtlinien (IEEE 802.11)
Richtlinien für öffentliche Schlüssel
Richtlinien für Softwareeinschränkung
Network Access Protection
IP-Sicherheitsrichtlinien auf Active Directory (SCH
Richtlinienbasierter QoS
Administrative Vorlagen: Vom lokalen Computer abgerufe
Einstellungen
Benutzerkonfiguration
Richtlinien
1
2
3
4
5
Keine Richtlinien für Softwareeinschränkung definiert
In diesem Gruppenrichtlinienobjekt wurden keine Richtlinien für Softwareeinschränkung definiert. Falls Sie Richtlinien für Softwareeinschränkung in diesem Gruppenrichtlinienobjekt definieren, werden diese die vererbten Richtlinieneinstellungen von anderen Gruppenrichtlinienobjekten außer Kraft setzen.
Klicken Sie im Menü "Aktion" auf "Neue Richtlinien für Softwareeinschränkung erstellen", um Richtlinien für Softwareeinschränkung zu definieren.
Hinweis: Nach dem Erstellen von Gruppenrichtlinienobjekten ist ein Neustart erforderlich.


Gruppenrichtlinienverwaltungs-Editor
Datei Aktion Ansicht ?
Programme von USB sperren [DC01.SCHULE.LOCAL] Richtlinie
Computerkonfiguration
Richtlinien
Softwareeinstellungen
Windows-Einstellungen
Skripts (Start/Herunterfahren)
Bereitgestellte Drucker
Sicherheitseinstellungen
Kontorichtlinien
Lokale Richtlinien
Ereignisprotokoll
Eingeschränkte Gruppen
Systemdienste
Registrierung
Dateisystem
Richtlinien für verkabelte Netzwerke (IEEE 802.3)
Windows-Firewall mit erweiterter Sicherheit
Netzwerklisten-Manager-Richtlinien
Drahtlosnetzwerkrichtlinien (IEEE 802.11)
Richtlinien für öffentliche Schlüssel
Richtlinien für Softwareeinschränkung
Neue Richtlinien für Softwareeinschränkung erstellen
Alle Aufgaben
Ansicht
Hilfe
Einstellungen
Benutzerkonfiguration
Richtlinien
Keine Richtlinien für Softwareeinschränkung definiert
In diesem Gruppenrichtlinienobjekt wurden keine Richtlinien für Softwareeinschränkung definiert. Falls Sie Richtlinien für Softwareeinschränkung in diesem Gruppenrichtlinienobjekt definieren, werden diese die vererbten Richtlinieneinstellungen von anderen Gruppenrichtlinienobjekten außer Kraft setzen.
Klicken Sie im Menü "Aktion" auf "Neue Richtlinien für Softwareeinschränkung erstellen", um Richtlinien für Softwareeinschränkung zu definieren.
Hinweis: Nach dem Erstellen von Gruppenrichtlinienobjekten ist ein Neustart erforderlich.
Erstellt Richtlinien für Softwareeinschränkung für dieses Gruppenrichtlinienobjekt.

Die Pfadregel
Die wohl in der Praxis am meisten benutzte Regel für Softwareeinschränkungen. Hier kann man als Administrator Pfade zum Dateisystem angeben, die einer bestimmten Regel unterzogen werden sollen. Auch möglich ist das Verwenden von Jokerzeichen wie dem Stern (*) für beliebig viele oder das Fragezeichen (?) für einzelne Zeichen möglich.

Hier einige Pfadbeispiele:

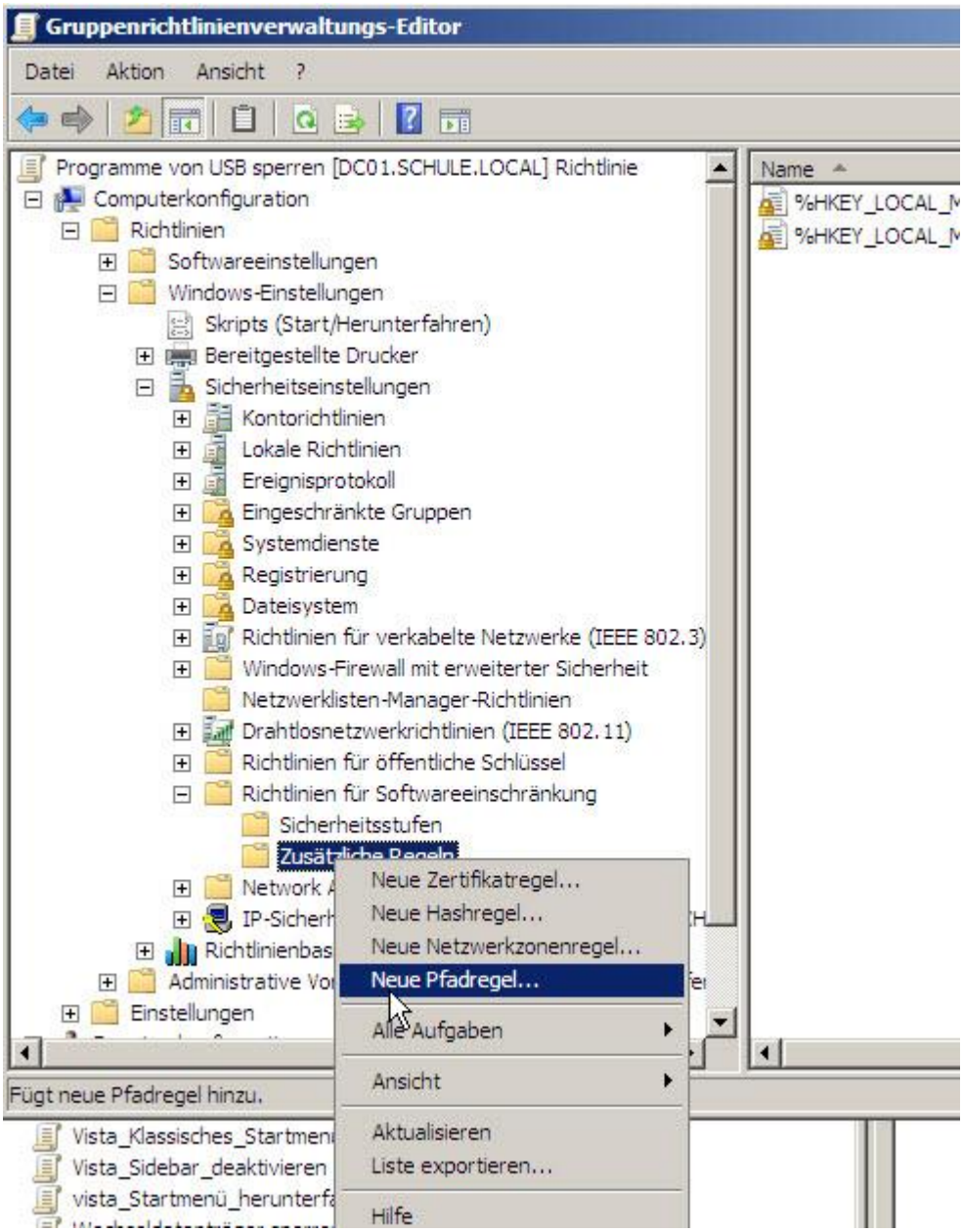
C:\Programme\meineApplikation*.doc
diese Pfadangabe wird alle DOC-Dateien im angegebenen Ordner treffen.

\\FileServer0??\meinShare\Dateien
dieser Pfad wird alle Dokumente und Dateien auf den Maschinen "Fileserver000" bis "Fileserver099" im Ordner "Dateien" treffen (aber auch "Fileserver0a3" oder "Fileserver08D" wären möglich). Für die Fragezeichen kann jeweils ein beliebiges Zeichen eingesetzt werden.

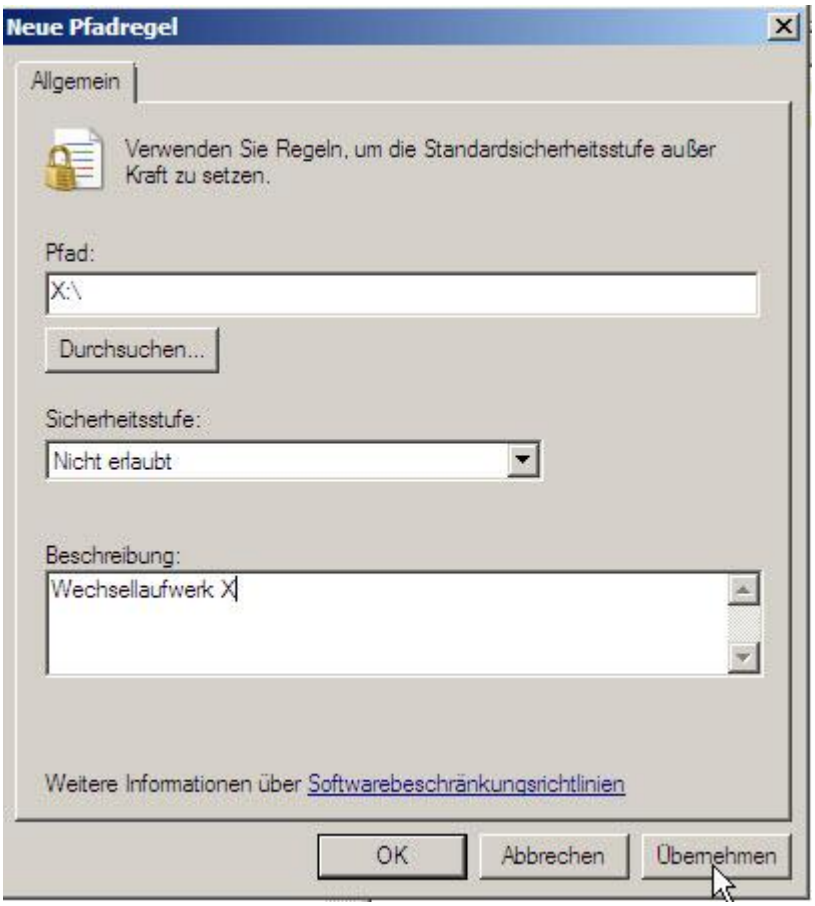
C:\temp\evil.*
dieser Pfad wird alle Dateien im Ordner "Temp" treffen, die den Namen "evil" tragen. Hierbei sorgt der Stern dafür, dass die Dateiendung egal ist.

Selbst Umgebungsvariablen können für die Pfadregeln verwendet werden:
%WINDIR%\system32*.vbs
alle Dateien mit der Dateieindung VBS im Ordner "%WINDIR%\system32 werden hier behandelt. %WINDIR% ist insofern interessant, als dass Windows in verschieden benannten Ordnern installiert worden sein kann ("Windows", "WINNT", …)

Auch ***%HOMEDRIVE%, %HOMEPATH% oder %PROGRAMFILES%***, sowie ***%TEMP%*** funktionieren einwandfrei.



Nun können, die vom USB Driveletter Manager benannten Laufwerke angeben werden. (z.B. x, y, z)



Natürlich kann man über diese Richtlinien auch bestimmte Programme erlauben, wenn z.B. firefox ausgeführt werden darf.

Natürlich gibt es auch eine Reihe von Drittanbieter Programme, die die Kontrolle von USB Wechseldatenträgern steuern. Diese sind aber meist kostenpflichtig.