

bi-Cube[®] Guideline

bi-Cube[®] USB-Blocker

Technologien Lösungen Trends Erfahrung



1	Ziel	3
2	Voraussetzungen und Lösungsansatz	3
2.1	Wie arbeitet der <i>bi-Cube[®]</i> USB-Blocker?	4
2.2	Wie sicher ist der <i>bi-Cube[®]</i> USB-Blocker?	5
3	Umsetzung	6
3.1	Programm-Installation	6
3.1.1	Systemvoraussetzungen	6
3.1.2	<i>bi-Cube[®]</i> USB-Blocker installieren	6
3.1.3	<i>bi-Cube[®]</i> USB-Blocker deinstallieren	7
3.2	Bedienung des Programms	8
3.2.1	Gruppen erzeugen	8
3.2.1.1	Vorüberlegungen	8
3.2.1.2	Gruppennamen ermitteln	9
3.2.1.3	Schreibzugriff einschränken	12
3.2.1.4	Namenskonventionen	13
3.2.1.5	Mitgliedschaften verwalten	13
3.2.1.5.1	So erstellen Sie eine lokale Gruppe	13
3.2.1.5.2	So löschen Sie eine lokale Gruppe	14
3.2.1.5.3	So fügen Sie ein Mitglied zu einer Gruppe hinzu	14
3.2.1.5.4	So entfernen Sie ein Mitglied aus einer Gruppe	14
3.2.1.6	Windows XP Home Edition	15
3.2.2	Konfigurieren des <i>bi-Cube[®]</i> USB-Blocker	15
3.2.2.1	<i>bi-Cube[®]</i> USB-Blocker Adminbenutzer	15
3.2.2.2	Einstellungen für die Gruppenkonfiguration	16
3.2.2.3	Einstellungen für die Log-Tätigkeit des <i>bi-Cube[®]</i> USB-Blocker	17
3.2.2.4	Einstellungen für die NDS-Unterstützung	18
3.2.2.5	Einstellungen für Zusatzparameter	19
3.2.3	Gruppenverwaltung im NDS	20
3.2.3.1	Verwendbare Gruppenkonstellationen	20
3.2.3.2	Konfigurationshinweise für die NDS-Nutzung	21
3.3	Installation per Softwareverteilung	22
3.4	Verwaltung des <i>bi-Cube[®]</i> USB-Blockers per Gruppenrichtlinien(GPO)	22
3.5	<i>bi-Cube[®]</i> USB-Blocker 30-Tage-Testversion	24
4	Ergebnisse - Beispielkonfiguration	25
4.1	Active Directory	25
4.2	NDS/eDirectory	28
4.3	Lokal	32
4.4	Sämtliche USB-Geräte deaktivieren	34
4.4.1	Deaktivieren aller USB-Geräteklassen	34
4.4.2	Deaktivieren des USB-Hubs	34
5	Erweiterung der Funktionen des <i>bi-Cube[®]</i> USB-Blocker mit <i>bi-Cube[®]</i> IPM	35
6	Hinweise	36
7	FAQ	36
	Abbildungsverzeichnis	37

1 Ziel

Wie kann ich mit **bi-Cube[®]** erreichen, dass im Unternehmen die Nutzung fast beliebiger Hardware kontrolliert werden kann?

2 Voraussetzungen und Lösungsansatz

USB-Geräte erreichen eine zunehmende Verbreitung und stellen neue Anforderungen an die Administratoren. Insbesondere die kleinen USB-Speichersticks eröffnen neue Dimensionen. Nicht nur, dass ihre Handhabung denkbar einfach ist und sie hervorragend für mobile Speicherung sensibler Daten geeignet sind, sie ermöglichen auch den schnellen und fast unbemerkbaren Datendiebstahl.

Wurden in der Vergangenheit vielfältige Maßnahmen ergriffen, um die Arbeitsplatz-PC's abzusichern z.B. Abschaltung oder Ausbau von CD-ROM und Disketten-Laufwerken, so greifen diese „einfachen“ (Hardware)-Schutzmaßnahmen bei z.B. USB-Speichersticks nicht. Hardwareseitig kann nicht zwischen den verschiedenen USB-Gerätetypen z.B. Drucker, Hub oder USB- Massenspeicher unterschieden werden.

Der **bi-Cube[®] USB-Blocker** in der Version 1.0 schuf erstmalig die Möglichkeit, die Nutzung der USB-Massenspeicher benutzerabhängig zu steuern.

Mit dem nun vorliegenden **bi-Cube[®] USB-Blocker** stehen Ihnen neue und umfangreiche Möglichkeiten zur Kontrolle der Nutzung fast beliebiger Hardware in Ihrem Unternehmen zur Verfügung.

2.1 Wie arbeitet der **bi-Cube[®]** USB-Blocker?

Die Arbeitsweise des **bi-Cube[®]** USB-Blocker ist denkbar einfach.

Jedes Gerät in Ihrem PC verfügt über diverse Eigenschaften. Eine Auswahl dieser Eigenschaften können Sie sich beispielsweise im Windows-Geräte-Manager anzeigen lassen.

1. Klicken Sie zum Öffnen des Geräte-Managers auf **Start**, und klicken Sie dann auf **Systemsteuerung**. Doppelklicken Sie auf **System**. Klicken Sie auf der Registerkarte **Hardware** auf **Geräte-Manager**.
2. Navigieren Sie in der angezeigten Struktur zu einem beliebigen Hardware-Gerät z.B. ein DVD/CD-Rom-Laufwerk Ihres Rechners.
3. Klicken Sie zum Anzeigen der Geräteeigenschaften im Menü auf **Aktion** und dann auf **Eigenschaften**.
4. Auf der Registerkarte **Details** können Sie sich eine Auswahl der Eigenschaften anzeigen lassen.

Einige dieser Eigenschaften identifizieren das Gerät eindeutig, andere beschreiben seine Zugehörigkeit zu verschiedenen Klassen, Services usw.

Mit dem **bi-Cube[®]** USB-Blocker können sowohl einzelne Geräte als auch eine Gruppe von Geräten über ihre Klassen-, Servicezugehörigkeit usw. überwacht werden.

Soll ein bestimmtes Gerät, eine Geräteklasse, ein Service usw. der Überwachung durch den **bi-Cube[®]** USB-Blocker unterliegen, genügt es, wenn auf dem Rechner oder im Netzwerk eine namensgleiche Gruppe existiert. Zugriff auf das Gerät erhalten dann nur noch Mitglieder dieser Gruppe.

Auf diese Weise ist auch der Zugriff der Benutzer auf interne Geräte, wie z.B. CD-ROM oder Diskettenlaufwerk, einschränkbar.

Der **bi-Cube[®]** USB-Blocker unterstützt die Verzeichnisdienste **Active Directory** und **Novell eDirectory (NDS)**. Die notwendigen Verbindungen werden nur bei Bedarf aufgebaut.

Das Programm wird auf allen zu überwachenden Rechnern installiert und dabei als Windows-Dienst eingerichtet. Der Start erfolgt automatisch mit dem Windows-Betriebssystem.

Hinweis:

Der USB-Blocker -Dienst gewährleistet die Kontrolle der Geräte. Während der Installation wird der Dienst so eingerichtet, dass nur Administratoren ihn beenden können.

Mit der Anmeldung eines Benutzers wird der **bi-Cube[®]** USB-Blocker aktiv:

- Er ermittelt die lokal oder im Netzwerk vorhandenen Gruppen sowie die Gruppen, in denen der angemeldete Benutzer Mitglied ist.
- Er speichert diese Informationen zusätzlich in Dateiform.
- Er überprüft die am Rechner angeschlossenen und installierten Geräte daraufhin, ob sie überwacht werden sollen und ob der Benutzer sie nutzen darf.
- Er sperrt optional den Bildschirm des Benutzers, bis das unzulässige Gerät wieder entfernt wurde oder die Sperre durch einen Administrator aufgehoben wurde.

2.2 Wie sicher ist der **bi-Cube[®]** USB-Blocker?

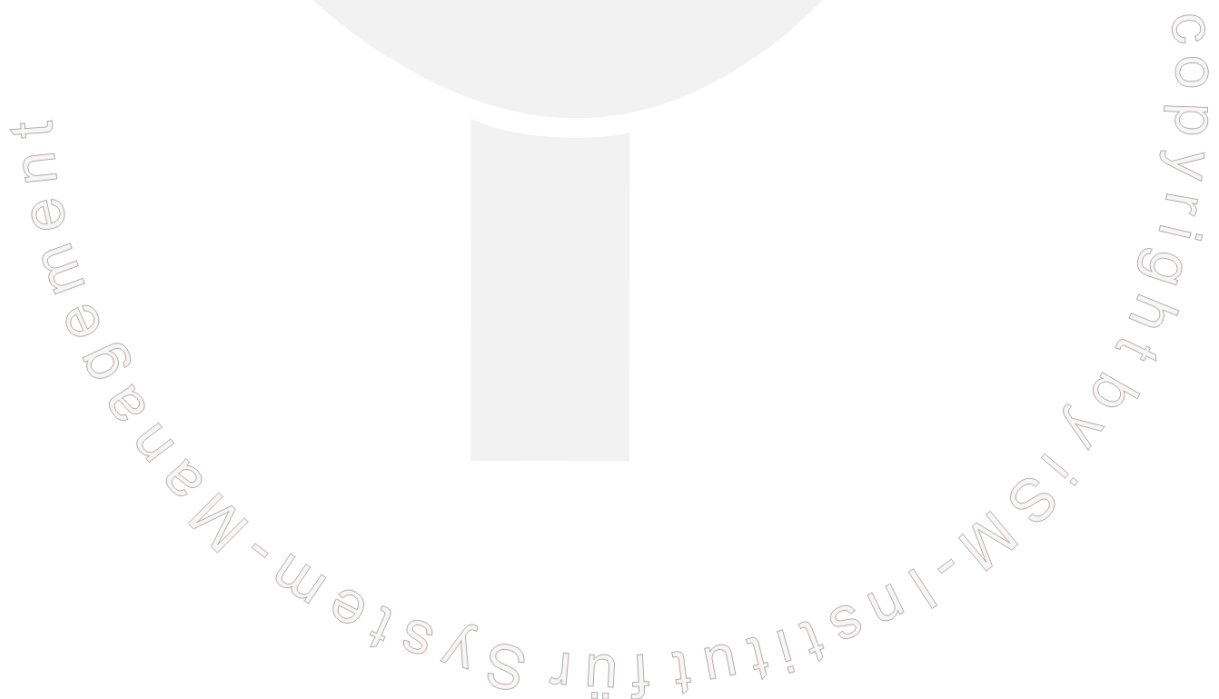
Alle Komponenten, die der **bi-Cube[®] USB-Blocker** benötigt, sind für den Standard-Benutzer zwar sichtbar jedoch nicht veränderbar.

Dazu gehören die Dienste „iSM USBBlockService“ und „iSM Drive Protect“, der Benutzer USBAdmin sowie die Dateien im Installationsverzeichnis.

Wir raten grundsätzlich davon ab, Benutzer mit Hauptbenutzer- bzw. Adminbenutzerrechten zu versehen. Diese beinhalten vielfältige Möglichkeiten Software zu deaktivieren bzw. zu umgehen.

Der Standard-Benutzer hat keine Möglichkeit, die Überwachungsfunktion des **bi-Cube[®] USB-Blocker zu umgehen.**

Zum Auswerfen oder Deaktivieren von nicht zugelassener Hardware wird der lokale Benutzer **USBAdmin** verwendet. Dieser wird während der Programminstallation erzeugt und er wird Mitglied der Gruppe der Administratoren. Um einen Missbrauch auszuschließen, erhält der USBAdmin bei jeder Installation ein neues Zufallspasswort.



3 Umsetzung

3.1 Programm-Installation

3.1.1 Systemvoraussetzungen

Der **bi-Cube[®] USB-Blocker** lässt sich auf folgenden Betriebssystemen installieren:

- Windows 7
- Windows Vista
- Windows XP Professional/Home
- Windows 2000 Professional
- Windows 2000 Server
- Windows Server 2003
- Windows Server 2008

Auf 64bit- Betriebssystemen werden die Basisfunktionen wie Sperren bzw. Blockieren von Geräten, aber vorerst nicht die Schreibschutzfunktion unterstützt.

Für die Verwaltung der Gruppen können folgende Systeme herangezogen werden:

- Active Directory
- Novell eDirectory (NDS)
- lokale Windows-Gruppen

Allgemein: Während der Installation werden 20 MB freier Speicherplatz benötigt.

Hinweise: **Windows NT wird nicht unterstützt!**
bi-Cube[®] USB-Blocker kann nicht auf einem Domänencontroller installiert werden!

3.1.2 **bi-Cube[®] USB-Blocker** installieren

Das Download-Paket umfasst die Dateien **USB-Blocker PLUS.exe**, **USB-Blocker PLUS.msi** und **isscript8.msi**. Die beiden MSI-Pakete dienen der Software-Verteilung (3.3), wobei die InstallShield Skript-Engine nur verteilt werden muss, wenn die Installation durch das **USB-Blocker PLUS.msi**-Paket einen entsprechenden Fehler im Anwendungsprotokoll des Zielsystems ausgibt.

Der **bi-Cube[®] USB-Blocker funktioniert ohne Serverkomponente. Die Installation des Programms auf einem Server ist deshalb nicht zwingend erforderlich. Es genügt die Konfigurationsoberfläche auf einer Administrationsstation zu installieren.**

Zur Installation des **bi-Cube[®] USB-Blocker** starten Sie die **USB-Blocker PLUS.exe**, wählen die Setup-Sprache und folgen den Anweisungen des Programms.

Wenn Sie vom Setup dazu aufgefordert werden, tragen Sie bitte die **Lizenznummer** in die dafür vorgesehenen Felder ein. Die Lizenznummer finden Sie im Mitteilungsschreiben, das Sie vom Institut für System-Management GmbH per E-Mail oder Post erhalten haben.

Für Testzwecke können Sie das Programm als 30-Tage-Testversion installieren.

Für die Konfiguration des **bi-Cube[®] USB-Blocker** steht Ihnen das Programm **USB-Blocker Admin** zur Verfügung. Wählen Sie zur Installation die entsprechende Option.

Das Setup des **bi-Cube[®] USB-Blockers**

- kopiert die notwendigen Dateien auf den Rechner,
- installiert und startet die Dienste „iSM USBBlockService“ und „iSM Drive Protect“,
- erzeugt den lokalen Benutzer USBAdmin mit Zufallspasswort und versieht ihn mit lokalen Administratorrechten und
- erstellt im Startmenü die Programmgruppe USB-Blocker und einige Menüeinträge.

Hinweis:

Die benötigten Dienste **iSM USBBlockService** und **iSM Drive Protect** werden zum Abschluss der Installation gestartet. Sind zu diesem Zeitpunkt auf dem Rechner oder im Netzwerk (Domäne) bereits Gruppen zur Überwachung eingerichtet, ist die Zugriffssteuerung sofort aktiv.

3.1.3 **bi-Cube[®] USB-Blocker deinstallieren**

Das Programm kann über das Windows-Dienstprogramm Software deinstalliert werden.

1. Klicken Sie zum Öffnen des Dienstprogramms Software auf **Start**, klicken Sie auf **Systemsteuerung** und klicken Sie dann auf **Software**.
2. Wählen Sie in der Liste der installierten Programme das Programm **USB-Blocker** aus und klicken Sie dann auf **Entfernen**.
3. Folgen Sie den Anweisungen des Programms.

3.2 Bedienung des Programms

Die Bedienung des Programms ist denkbar einfach und besteht aus 3 Schritten:

1. Gruppen erzeugen
Für jedes Gerät, jede Klasse, Service usw. welche(s) überwacht werden soll, brauchen Sie lediglich eine Gruppe mit der entsprechenden Bezeichnung auf dem Rechner bzw. in der Domäne erzeugen.
Sobald diese Gruppe existiert, erlaubt der **bi-Cube[®] USB-Blocker** nur noch Mitgliedern dieser Gruppe den notwendigen Zugriff.
2. Mitgliedschaften verwalten
Durch das Hinzufügen oder Entfernen eines Benutzers zu den angelegten Gruppen erlauben bzw. verweigern Sie den Benutzern die Nutzung der überwachten Geräte.
3. **bi-Cube[®] USB-Blocker** konfigurieren
Auf die Arbeitsweise des Dienstes **USB-Blocker** kann durch verschiedene Konfigurationen Einfluss genommen werden. Hierzu zählen
 - o das Vergeben von Usern für die Gruppenabfrage,
 - o das Definieren der Gruppenpräfixe,
 - o die Einstellungen für die Logtätigkeit,
 - o das Aktivieren und Konfigurieren der NDS Unterstützung.

3.2.1 Gruppen erzeugen

Bevor Sie Gruppen zur Überwachung von Geräten anlegen, entwickeln Sie Ihre Strategie zur Überwachung und Kontrolle der Hardware.

3.2.1.1 Vorüberlegungen

Dabei sind folgende Überlegungen wichtig:

1. Jedes Gerät lässt sich verschiedenen Gruppen zuordnen.
2. Um ein Gerät zu sperren, muss mindestens **eine** dieser Gruppen vorhanden sein.
! Allein die Existenz einer dieser Gruppen führt zur Sperrung von Geräten!
3. Um einem Benutzer die Nutzung eines überwachten Gerätes zu erlauben, muss er Mitglied mindestens **einer** dieser Gruppen sein.
4. Gruppen können eindeutig, also nur für ein Gerät zutreffend, oder übergreifend sein, also für mehrere Geräte zutreffend.
5. Zu jedem angeschlossenen Gerät werden durch den **bi-Cube[®] USB-Blocker** fünf Eigenschaften ermittelt:
 - a) Geräteservice
 - b) Geräteklasse
 - c) Geräteklassenbeschreibung
 - d) Geräteanzeigename
 - e) Geräte-ID
6. Um die eindeutige Identifikation von Geräten zu gewährleisten, können diese Eigenschaften kombiniert werden.

7. Durch Wildcards wird ermöglicht, dass z.B. verschiedene USB-Sticks desselben Chipsatzherstellers mit nur einer Gruppe freigegeben werden können. Um die Wildcards „Stern“ und „Fragezeichen“ auszudrücken, können Zeichenkombinationen definiert werden.
8. Interne Geräte werden durch den **bi-Cube[®] USB-Blocker** deaktiviert. Hierbei ist jedoch zu beachten, dass die Geräte-ID von scheinbar unabhängigen Systemgeräten identisch sein kann. Dies kann zu einer unbeabsichtigten Gerätesperrung führen. Empfehlenswert ist daher eine Sperrung **nicht** über die Geräte-ID, sondern über die Geräteklassen bzw. Geräteservices.

Beachten Sie, dass das Sperren von internen Hardwarekomponenten zu einem eventuellen Systemausfall führen kann. Bitte testen Sie daher Ihre Einstellungen vorher an einem nicht im Netz befindlichen Rechner.

Weiterhin gibt es die Möglichkeit, zwei Sondergruppen einzurichten.

1. HW_TRUSTED
 - Mitglieder dieser Gruppe dürfen ohne Einschränkung alle Geräte benutzen.
 - Die Existenz dieser Gruppen allein bewirkt nichts.
2. HW_NOTRUSTED
 - Für Mitglieder dieser Gruppe werden ohne Ausnahme alle Geräte gesperrt. Das Benutzen von Geräten muss explizit erlaubt werden.
 - Mitglieder dieser Gruppe, die auch gleichzeitig Mitglied in der für das entsprechende System angelegten SystemHardwareLock Gruppe sind, können an dem Rechner keinerlei Veränderungen an der Hardware vornehmen.
 - Die Existenz dieser Gruppen allein bewirkt nichts.
 - Hinweis:
ALLE Geräte heißt in diesem Fall wirklich **ALLE**. Dies betrifft nicht nur USB, HDD, CD-ROM usw. sondern Mouse, Tastatur, Display, also alles was im Geräte-Manager aufgelistet wird.

Der Erfolg Ihrer Strategie hängt von der wohlüberlegten Kombination der Möglichkeiten ab.

Beispielsweise können Sie durch Erzeugung einer Gruppe die USB-Massenspeicher global sperren und dann durch spezielle Gerätegruppen einzelne USB-Massenspeicher zulassen.

3.2.1.2 Gruppennamen ermitteln

Für die Ermittlung der notwendigen Gruppennamen steht Ihnen das Programm **USB-Blocker Admin** zur Verfügung.

Starten Sie das Programm USB-Blocker Admin:

Klicken Sie zum Öffnen des Programms USB-Blocker Admin auf **Start**, klicken Sie auf **alle Programme**, wählen Sie den Eintrag **USB-Blocker** und klicken Sie dann auf **USB-Blocker Admin**.



Abbildung 1 USB-Blocker Admin

Im linken Teil der Programmoberfläche sehen Sie die Gerätestruktur der in Ihrem Rechner installierten und angeschlossenen Geräte. Sie entspricht in ihrem Aufbau dem Windows Geräte-Manager.

Über die Symbolleiste können Sie

- die Sortierung und Art der Anzeige der Struktur verändern,
- die Anzeige manuell aktualisieren und
- sich mit einem Rechner Ihres Netzwerkes remote verbinden.

Die Anzeige für die lokal vorhandenen Geräte wird bei jeder Hardwareänderung automatisch aktualisiert.

→ Schließen Sie die Geräte, die Sie überwachen möchten, an Ihrem Rechner an oder verbinden Sie sich remote mit einem Rechner, an dem das Gerät angeschlossen ist.

→ Navigieren Sie in der Struktur zu jedem Gerät, für das Sie die Gruppennamen ermitteln möchten.

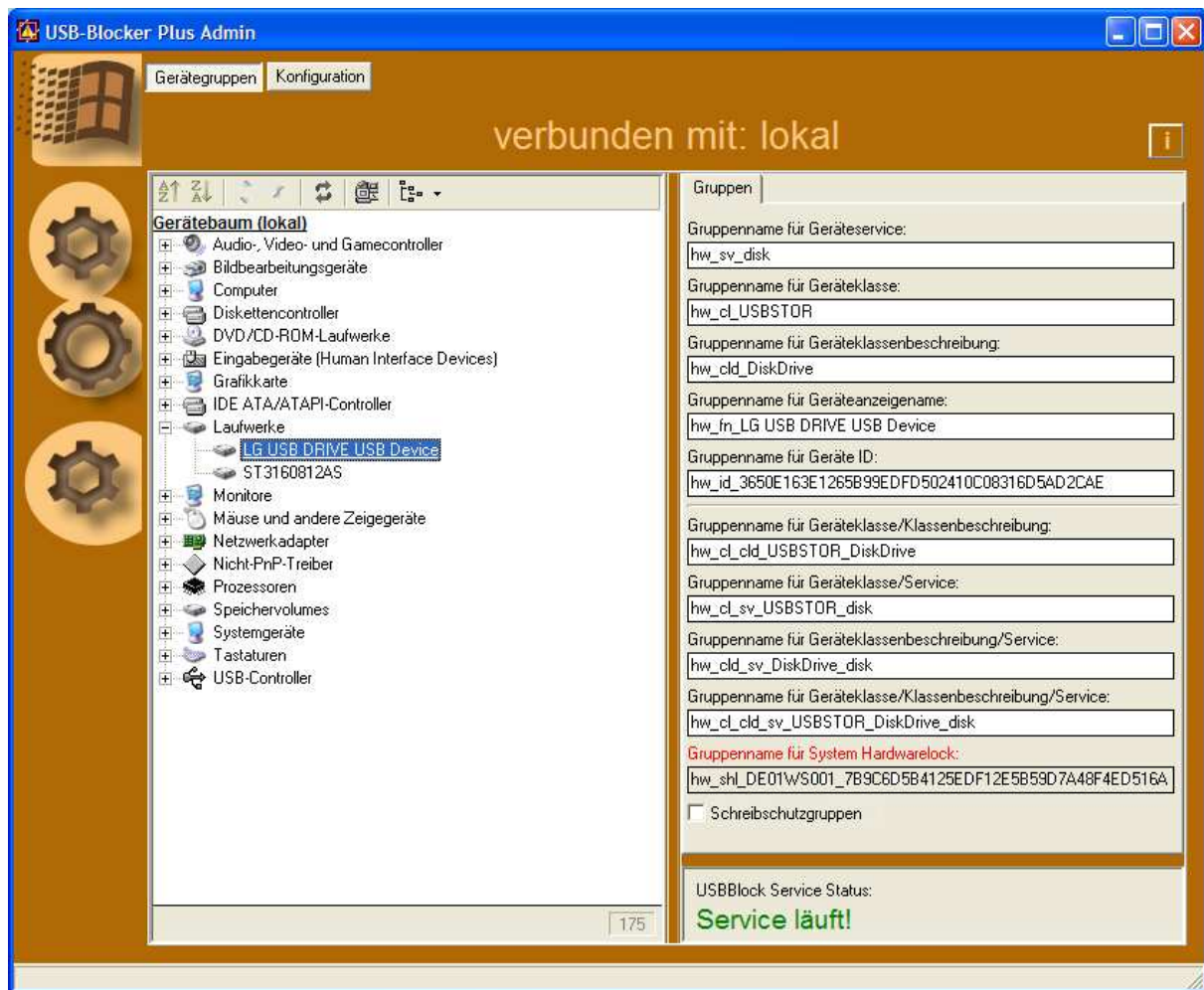


Abbildung 2 Gerätedetailanzeige

In der Detailanzeige auf der rechten Seite werden Ihnen die möglichen Gruppennamen angezeigt.

Die ersten fünf Gruppennamen werden direkt aus den Geräteeigenschaften

1. Geräteservice
2. Geräteklasse
3. Geräteklassenbeschreibung
4. Geräteanzeigename
5. Geräte-ID

gebildet. Die vier weiteren Gruppennamen sind Kombinationen aus diesen Eigenschaften.

Z.B. ein USB-Speicherstick erscheint in der Auflistung

1. als USB-Massenspeicher unter USB-Controller
2. als <Anzeigename> unter Laufwerke
3. als Standardvolume unter Speichervolumen

Um diese Zusammenhänge besser sichtbar zu machen, wechseln Sie Strukturansicht und lassen sich die **Geräte nach Verbindung anzeigen**.

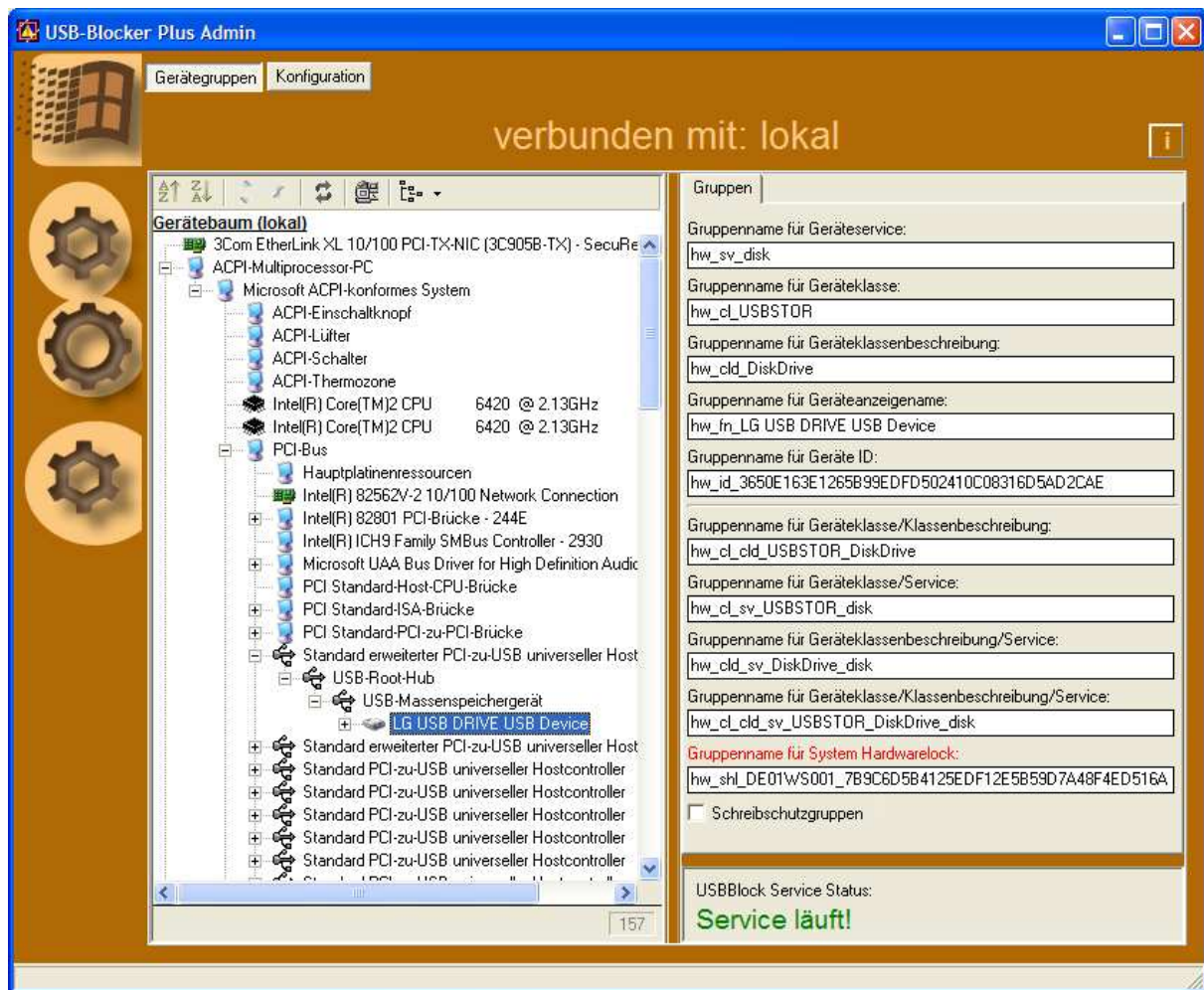


Abbildung 3 Geräte nach Verbindung

Prinzipiell ist jeder Eintrag ein eigenes Gerät und kann somit gesperrt werden. Geräte, die von diesem abhängig sind, sind dann ebenfalls von der Sperrung betroffen, es sei denn, Sie haben solche abhängigen Geräte wieder freigegeben. Wählen Sie den oder die Gruppennamen, der Ihrer geplanten Sperrstrategie am besten entspricht.

3.2.1.3 Schreibzugriff einschränken

Mit dem **bi-Cube[®] USB-Blocker** ist es auch möglich, den schreibenden Zugriff auf einen Datenträger zu verhindern. Wenn ein Gerät in den schreibgeschützten Zustand versetzt werden kann, wird dies durch die Checkbox **Schreibschutzgruppen** signalisiert.

Bei Aktivierung dieser Option werden die angezeigten Gruppennamen durch das Anhängsel _01 ergänzt. Wenn der **bi-Cube[®] USB-Blocker** ein Gerät findet, für das eine Schreibschutzgruppe existiert, können auf das entsprechende Gerät keine Daten geschrieben werden.

Für Mitglieder solch einer Schreibschutzgruppe wird der Schreibschutz aufgehoben.

Für Mitglieder einer normalen Sperrgruppe ist nur der lesende Zugriff möglich.

Existiert keine normale Sperrgruppe für das gleiche Gerät, haben alle, die nicht Mitglied in der Schreibschutzgruppe sind, nur Leseberechtigung.

3.2.1.4 Namenskonventionen

Im **USB-Blocker Admin** werden Ihnen die Gruppennamen standardmäßig mit einem Präfix angezeigt. Für die einzelnen Eigenschaften sind das

- | | |
|------------------------------|--------|
| 1. Geräteservice | hw_sv |
| 2. Geräteklasse | hw_cl |
| 3. Geräteklassenbeschreibung | hw_cld |
| 4. Geräteanzeigename | hw_fn |
| 5. Geräte-ID | hw_id |

Für die Kombinationen der Gruppennamen sind auch die Präfixe entsprechend kombiniert.

Diese Präfixe sind wahlfrei und sollen die Gruppenverwaltung erleichtern. Sie können diese Präfixe in der USBBlock.ini Ihren Bedürfnissen anpassen.

3.2.1.5 Mitgliedschaften verwalten

Die Erlaubnis zur Nutzung der Hardwaregeräte wird über die Mitgliedschaft in lokalen oder Domänengruppen gesteuert. Um einem Benutzer diese Erlaubnis zu erteilen, müssen Sie ihn zum Mitglied dieser lokalen Gruppe bzw. der Domänengruppe machen.

Sie müssen möglicherweise als **Administrator** oder als Mitglied der Gruppe **Administratoren** angemeldet sein, um einige dieser Aufgaben ausführen zu können.

Exemplarisch wird hier das Vorgehen unter Benutzung der Computerverwaltung in XP Professional beschrieben.

In den verschiedenen Betriebssystemen gibt es eine Vielzahl von Verwaltungs- und Befehlszeilenprogrammen, mit deren Hilfe Sie diese Aufgabe erledigen können. Konsultieren Sie dazu die Hilfe des jeweiligen Betriebssystems.

3.2.1.5.1 So erstellen Sie eine lokale Gruppe

1. Öffnen Sie die **Computerverwaltung**.
2. Navigieren Sie in der Konsolenstruktur zu **Gruppen**.
 - Computerverwaltung
 - Systemprogramme
 - Lokale Benutzer und Gruppen
 - Gruppen
3. Klicken Sie auf **Aktion**, und klicken Sie dann auf **Neue Gruppe**.
4. Geben Sie im Feld **Gruppenname** einen Namen für die neue Gruppe ein.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

Anmerkungen

- Klicken Sie zum Öffnen der Computerverwaltung auf **Start**, und klicken Sie dann auf **Systemsteuerung**. Klicken Sie auf **Leistung und Wartung**, klicken Sie auf **Verwaltung** und doppelklicken Sie dann auf **Computerverwaltung**.
- Der Name einer lokalen Gruppe darf mit keinem anderen Gruppen- oder Benutzernamen auf dem verwalteten Computer identisch sein. Der Name kann bis zu 256 Klein- oder Großbuchstaben und Zeichen mit Ausnahme der folgenden enthalten: " / \ [] ; | = , + * ? < >

- Der Name der Domänengruppen kann alle Unicode-Zeichen enthalten, mit Ausnahme der speziellen LDAP-Zeichen gemäß RFC 2253: führendes und nachfolgendes Leerzeichen sowie die Sonderzeichen # , + " \ < > ;
- Ein Gruppenname darf nicht ausschließlich aus Punkten (.) oder Leerzeichen bestehen.

3.2.1.5.2 So löschen Sie eine lokale Gruppe

1. Öffnen Sie die **Computerverwaltung**.
2. Navigieren Sie in der Konsolenstruktur zu **Gruppen**.
 - Computerverwaltung
 - Systemprogramme
 - Lokale Benutzer und Gruppen
 - Gruppen
3. Klicken Sie mit der rechten Maustaste auf die zu löschende Gruppe und klicken Sie dann auf **Löschen**.

3.2.1.5.3 So fügen Sie ein Mitglied zu einer Gruppe hinzu

1. Öffnen Sie die **Computerverwaltung**.
2. Navigieren Sie in der Konsolenstruktur zu **Gruppen**.
 - Computerverwaltung
 - Systemprogramme
 - Lokale Benutzer und Gruppen
 - Gruppen
3. Klicken Sie mit der rechten Maustaste auf die Gruppe, zu der Sie ein Mitglied hinzufügen möchten, zeigen Sie auf **Alle Tasks**, klicken Sie auf **Mitglied hinzufügen**, und klicken Sie dann auf **Hinzufügen**.
4. Klicken Sie auf **Suchen in**, um eine Liste von Domänen anzuzeigen, aus denen Benutzer und Gruppen zur Gruppe hinzugefügt werden können.
5. Klicken Sie unter **Pfad** auf die Domäne mit den Benutzern und Computern, die Sie hinzufügen möchten und klicken Sie dann auf **OK**.
6. Geben Sie im Feld **Name** den Namen des Benutzers oder der Gruppe ein, den/die Sie zur Gruppe hinzufügen möchten und klicken Sie dann auf **OK**.

Wenn Sie die hinzugefügten Benutzer- oder Gruppennamen überprüfen möchten, klicken Sie auf **Namen überprüfen**.

3.2.1.5.4 So entfernen Sie ein Mitglied aus einer Gruppe

1. Öffnen Sie die **Computerverwaltung**.
2. Navigieren Sie in der Konsolenstruktur zu **Gruppen**.
 - Computerverwaltung
 - Systemprogramme
 - Lokale Benutzer und Gruppen
 - Gruppen
3. Klicken Sie mit der rechten Maustaste auf die Gruppe, zu der Sie ein Mitglied hinzufügen möchten, zeigen Sie auf **Alle Tasks**, klicken Sie auf **Mitglied hinzufügen** und klicken Sie dann auf **Hinzufügen**.
4. Wählen Sie im Feld **Mitglieder** den Benutzer oder die Gruppe aus und klicken Sie dann auf **Entfernen**.

3.2.1.6 Windows XP Home Edition

Unter Windows XP Home stehen die benötigten Verwaltungskonsolen nicht zur Verfügung. Sie können für die Gruppenverwaltung stattdessen den **net-Befehl** verwenden.

- Prüfen der vorhandenen lokalen Gruppen:

```
net localgroup
```

- Anlegen einer USB-Blocker Gerätegruppe:

```
net localgroup usb-blocker-gruppe /add
```

- Hinzufügen eines/einer Benutzers/Gruppe zu einer USB-Blocker Gerätegruppe:

```
net localgroup usb-blocker-gruppe Benutzername/Gruppe /add
```

- Überprüfung der Mitglieder der USB-Blocker Gerätegruppe:

```
net localgroup usb-blocker-gruppe
```

3.2.2 Konfigurieren des **bi-Cube[®] USB-Blocker**

Im **USB-Blocker Admin** kann zwischen der Ansicht für die Sperrgruppenermittlung und Dienstkonfiguration umgeschaltet werden.

Wenn Sie remote mit einem Rechner verbunden sind, können Sie sowohl die Gerätegruppen als auch die Konfiguration des **bi-Cube[®] USB-Blockers** des Remote-Computers einsehen und ändern.

Wichtig: Für die Konfiguration muss das Programm mit lokalen Admin-Rechten gestartet werden.



Abbildung 4 Umschalten der Programmansichten

3.2.2.1 **bi-Cube[®] USB-Blocker Adminbenutzer**

In diesem Bereich kann der vom **bi-Cube[®] USB-Blocker** verwendete lokale Windows-User geändert werden. Dieser Service-Account wird beim Installieren auf dem PC durch das Setup erstellt und mit einem Zufallspasswort versehen. Er besitzt administrative Rechte und wird benötigt, um beim Sperren von Geräten diese aus dem System entfernen zu können.

Der vom **bi-Cube[®] USB-Blocker** verwendete Benutzer kann geändert werden. Es muss nur darauf geachtet werden, dass dieser lokale administrative Rechte besitzt. Es können lokale und Domänen-User verwendet werden. Das Ändern des Adminbenutzers ist optional.

Wichtig: Das Ändern dieser Daten ist nur in sehr speziellen Szenarien nötig und kann dazu führen, dass der **bi-Cube[®] USB-Blocker nicht mehr richtig funktioniert.**

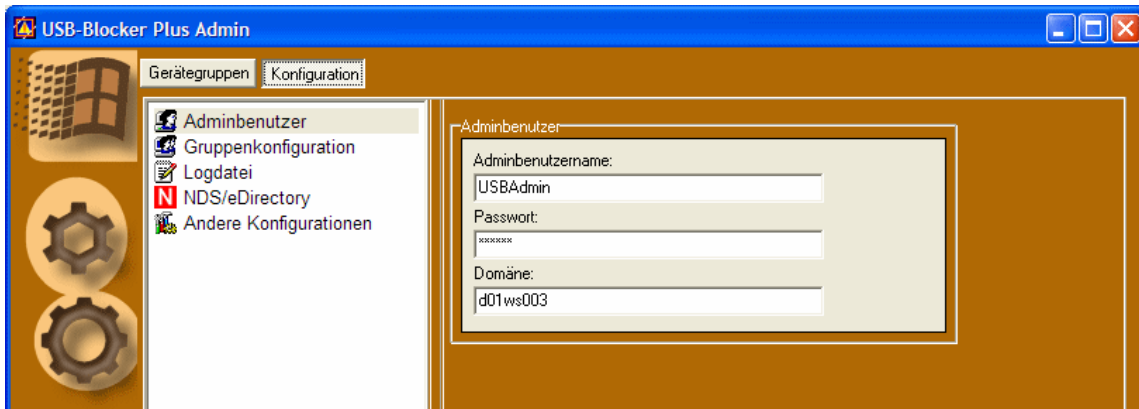


Abbildung 5 Einstellungen für den USB-Blocker Admin User

3.2.2.2 Einstellungen für die Gruppenkonfiguration

Alle verwendeten Gruppen für den **bi-Cube[®] USB-Blocker** richten sich nach einem einstellbaren Schema. Für alle Gruppen ist das feste **Präfix** bereits vorkonfiguriert. Diese Gruppenpräfixe können in diesem Teil des USB-Blocker Admin an eigene Bildungsregeln für Gruppen angepasst werden. Das Ändern dieser Einstellungen ist optional. Wir empfehlen, diese Einstellungen unverändert zu lassen.

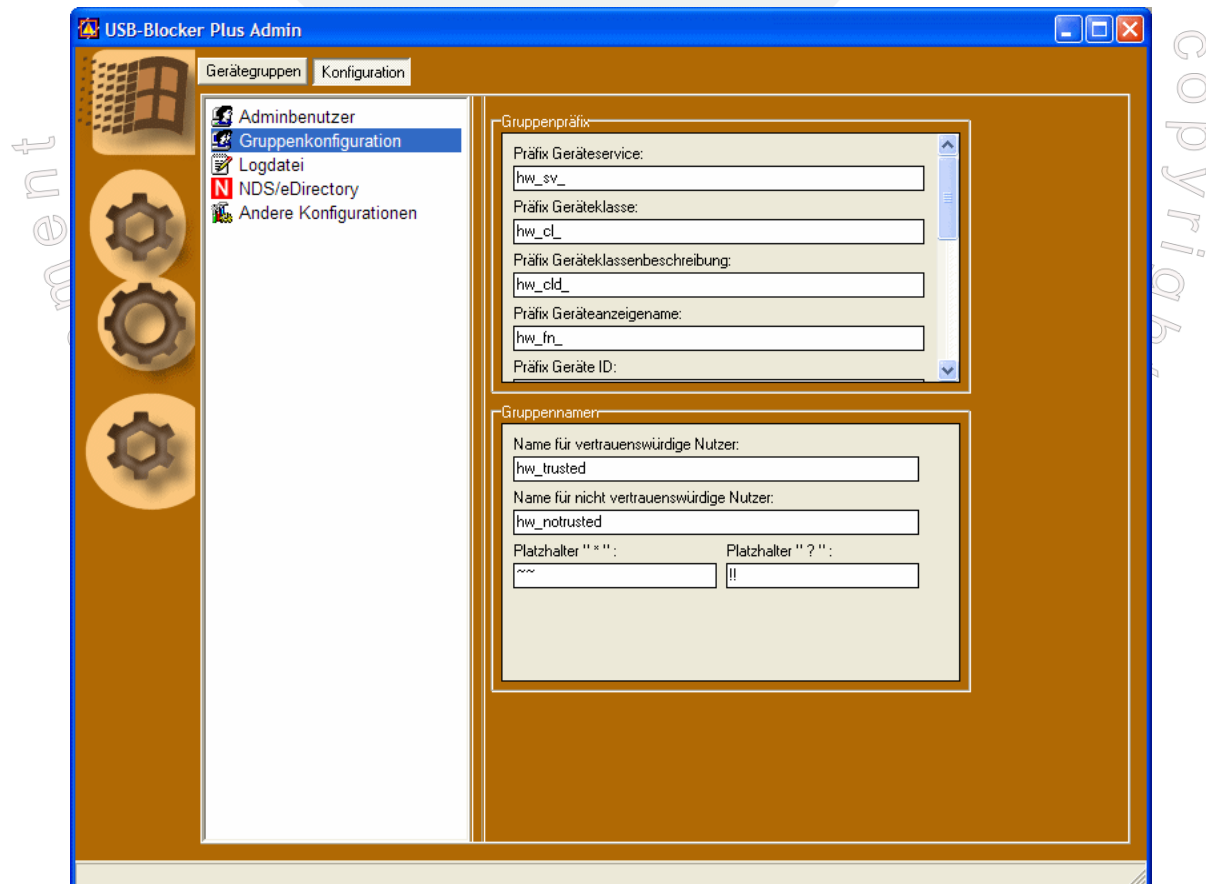


Abbildung 6 Einstellungen für die Gruppenkonfiguration

3.2.2.3 Einstellungen für die Log-Tätigkeit des **bi-Cube[®] USB-Blocker**

Unter diesem Punkt des Admin Tools kann die Log-Tätigkeit des **bi-Cube[®] USB-Blockers** konfiguriert werden.

Bei Aktivierung dieser Option werden alle Aktivitäten des **bi-Cube[®] USB-Blockers** protokolliert. Dazu gehören der angemeldete Benutzer, alle ermittelten Sperrgruppen, die Sperrgruppen, in denen der angemeldete Benutzer Mitglied ist, und alle den **bi-Cube[®] USB-Blocker** betreffenden Ereignisse wie z.B. das Einstecken eines USB-Gerätes.

Die Daten werden im csv-Format in die angegebene Datei gespeichert. Name und Pfad der Log-Datei können eigenen Vorstellungen angepasst werden.

Zusätzlich bietet der **bi-Cube[®] USB-Blocker** die Möglichkeit, alle Logdaten zentral in einer Datenbank zu speichern. Dazu müssen Servername und Port des ZAM-Server-Dienstes angegeben werden. Dieses Feature ist nur bei Verwendung der **bi-Cube[®]**-Erweiterung verfügbar.

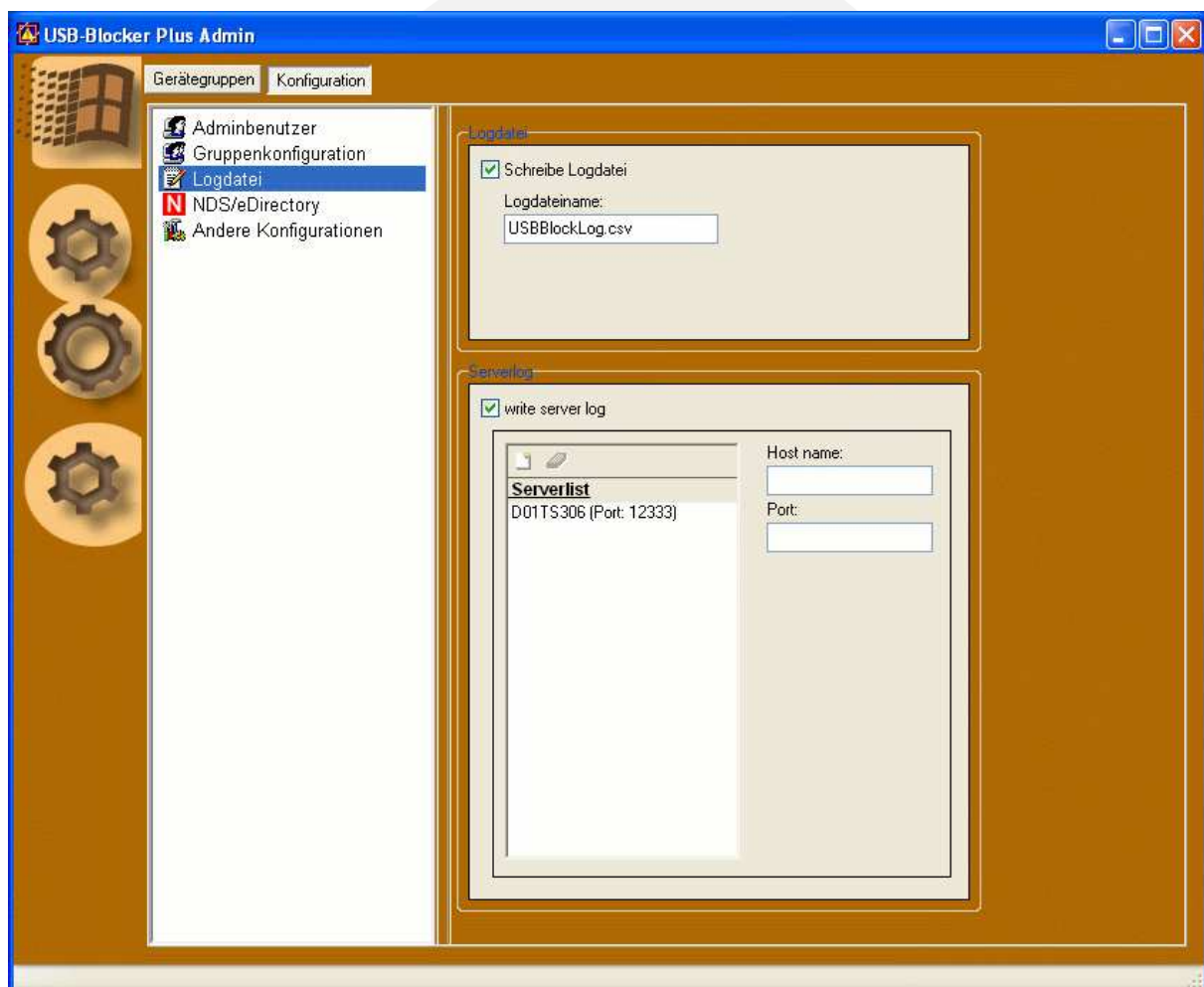


Abbildung 7 Einstellungen für die Log-Tätigkeit

3.2.2.4 Einstellungen für die NDS-Unterstützung

Die in dieser Ansicht dargestellten Einstellungen sind Voraussetzung für eine korrekte Zusammenarbeit des **bi-Cube[®] USB-Blockers** mit dem **NDS/eDirectory**. Nach der Installation des **bi-Cube[®] USB-Blockers** ist die Option **benutze Novell** standardmäßig deaktiviert.

Nach dem Aktivieren der Option stehen folgende Konfigurationsmöglichkeiten zu Verfügung:

a) Nutze Adminbenutzer für die NDS-Verbindung (ZEN)

Bei der Verwendung von ZENworks zur Softwareverteilung sollte diese Option aktiviert sein, da es sonst zu Problemen im Zusammenspiel mit dem ZENworks-Client kommen kann. Durch die Aktivierung dieser Option wird der im USB-Blocker Admin definierte Adminbenutzer zum Aufbau der Verbindung genutzt.

b) Gruppenabfragen unter diesem Benutzer-Account durchführen

Hier kann optional ein definierter Benutzer-Account angegeben werden, mit dessen Rechten alle notwendigen Abfragen im NDS ausgeführt werden.

c) Nutze Gruppenfilter Benutzer (NDS)

Durch das optionale Aktivieren des Gruppenfilter Benutzers wird der Suchvorgang zur Ermittlung der Gruppen im NDS verkürzt. Bei der Aktivierung dieser Option werden die Gruppenmitgliedschaften des hier angegebenen Benutzerkontos als Sperrgruppen genutzt. Ist der Gruppenfilter Benutzer nicht Mitglied in einer Gruppe, kann diese nicht zum Sperren herangezogen werden.

Die Verwendung dieser Option wird empfohlen.

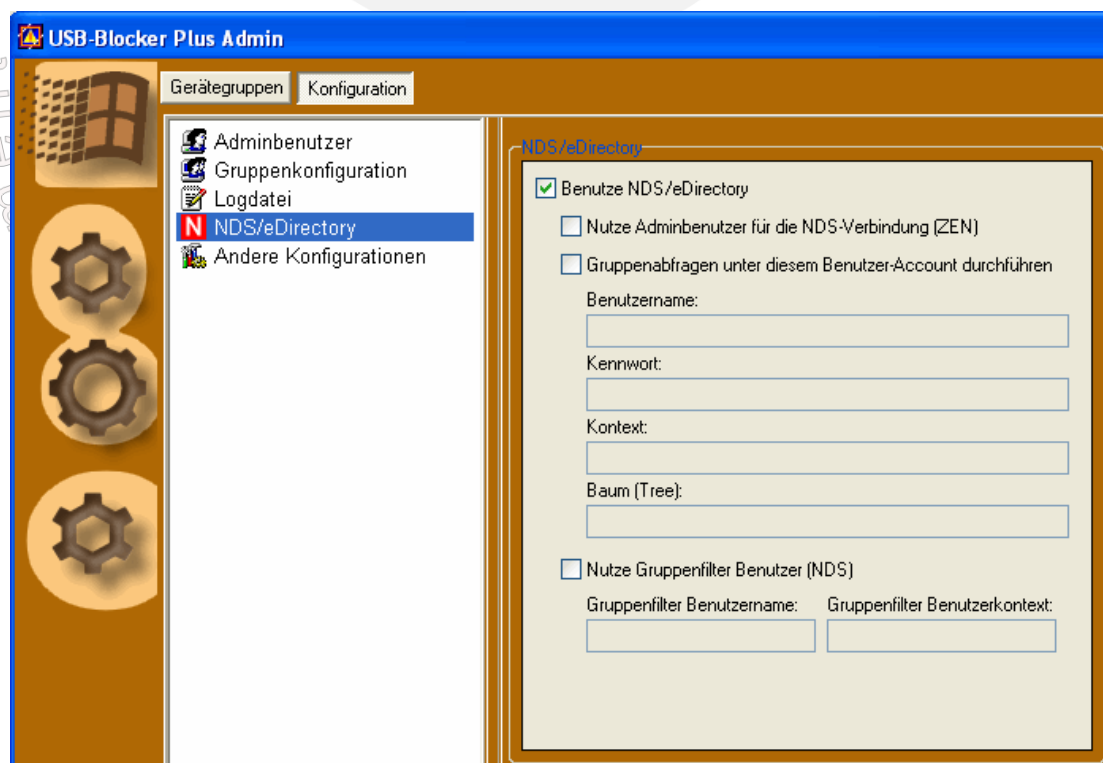


Abbildung 8 Einstellungen für die NDS/eDirectory Unterstützung

3.2.2.5 Einstellungen für Zusatzparameter

Die Optionen aus dem Bereich **Andere Konfiguration** haben folgende Bedeutung:

- a) Das **Aktualisieren der Gruppen bei Geräte- bzw. Datenträgerwechsel** bedeutet, dass der **bi-Cube[®] USB-Blocker** bei jedem Hinzukommen oder Entfernen von Geräten oder Datenträgern die Gruppenkonfiguration aktualisiert. Dabei werden die im AD/NDS bzw. lokal vorhandenen Gruppen neu eingelesen. Dies ist sinnvoll, wenn sich die Usermitgliedschaften in den Gruppen häufig ändern. Es kann dadurch vermieden werden, dass der User sich zum Aktualisieren erneut anmelden muss.
- b) Die Option **Vertraue Administratoren** dient dazu, die Blockfunktion für User mit administrativen Rechten unabhängig der vorhandenen Gerätegruppen zu deaktivieren.
- c) Die Option **Sperrbildschirm anzeigen** aktiviert den Sperrbildschirm, der für die Dauer des Geräteauswurfs erscheint. Sie ist standardmäßig aktiviert.
- d) Der Konfigurationspunkt **Generiere Geräte ID aus** dient zur Einstellung des Erzeugungsalgorithmus' der Geräte-ID-Gruppe. In seltenen Fällen kann es vorkommen, dass unterschiedliche externe Geräte die gleiche ID durch Windows zugewiesen bekommen. In diesem Fall ist es notwendig, die Identifizierung dieser Geräte weiter zu verfeinern. Voreingestellt ist die Generierung der Geräte-ID-Gruppe aus der **iSeriennummer**. Sollte diese Einstellung für eine genaue Identifizierung nicht ausreichen, kann durch das Hinzufügen weiterer Geräte Merkmale die Geräte-ID-Gruppe eindeutiger gebildet werden. Bei Punkt 2 werden neben der iSeriennummer noch die **Vendor ID** und **Produkt ID** für die Generierung der Geräte-ID verwendet. Bei Punkt 3 wird zusätzlich der Gerätenamen mit einbezogen. Bei Punkt 4 werden bei Massenspeichergeräten die Partitionsinformationen für die Generierung der Geräte-ID mit einbezogen.
- e) Aktivieren Sie **Verwende lokale Hardwaregruppen**, wenn lokal angelegte Gerätegruppen auch berücksichtigt werden sollen. Es wird empfohlen, diese Option bei Verwendung von AD oder Novell zu deaktivieren.
- f) Aktivieren Sie **Suche Hardwaregruppen im Active Directory**, wenn Sie die Gerätegruppen zentral im AD verwalten wollen.
- g) Durch das optionale Aktivieren **Nutze Gruppenfilter Benutzer (ADS)** wird der Suchvorgang zur Ermittlung der Gruppen im Active Directory verkürzt. Bei der Aktivierung dieser Option werden die Gruppenmitgliedschaften des hier angegebenen Benutzerkontos als Sperrgruppen genutzt. Ist der **Gruppenfilter Benutzername/-domäne** nicht Mitglied in einer Gruppe, kann diese nicht zum Sperren herangezogen werden. Die Verwendung dieser Option wird empfohlen.
- h) Mit dem Button **Export Config...** können Sie die aktuelle Konfiguration in eine reg-Datei exportieren, die für die Softwareverteilung oder das manuelle Übertragen der Konfiguration benötigt wird.

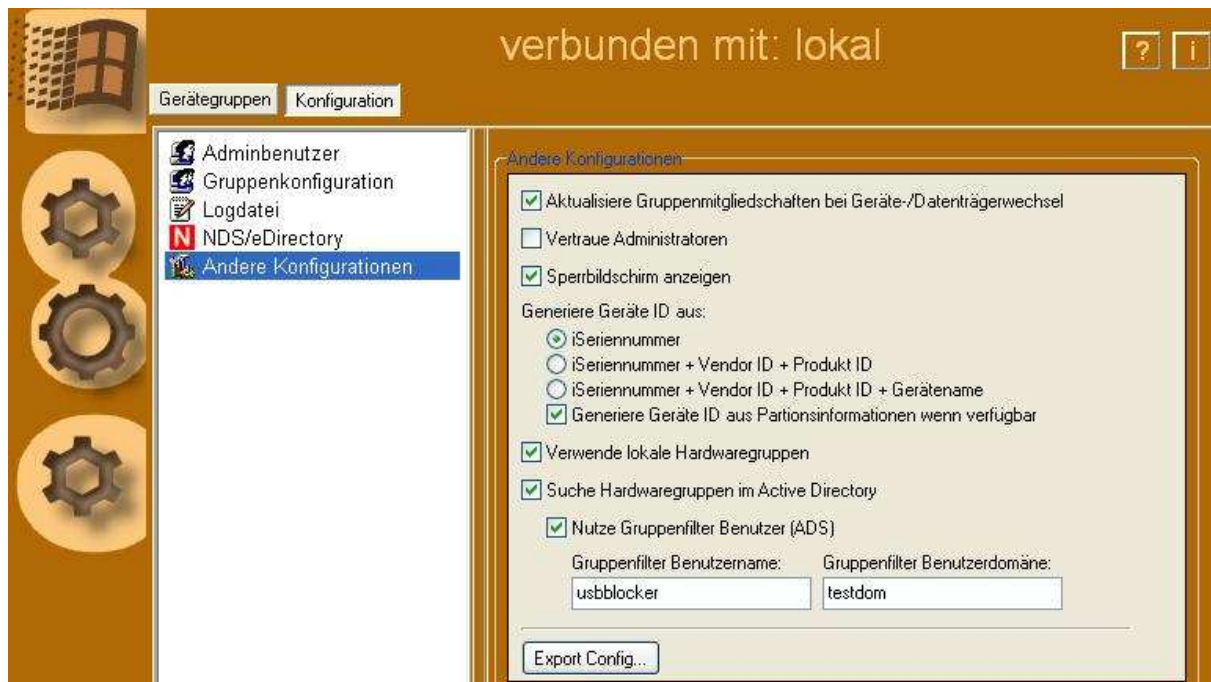


Abbildung 9 Einstellungen der Zusatzparameter

3.2.3 Gruppenverwaltung im NDS

Nach Aktivierung der Option zu Anbindung des **bi-Cube[®] USB-Blocker** an das **NDS** und Konfiguration der in Punkt 3.2.2.4 beschriebenen Optionen, liest der **bi-Cube[®] USB-Blocker** entsprechende Benutzergruppen im NDS aus. Falls der **Gruppenfilter Benutzername/-domäne** nicht verwendet werden soll, wird nachfolgend erklärt, welche Varianten von Zugehörigkeiten der User in den Gruppen möglich sind.

3.2.3.1 Verwendbare Gruppenkonstellationen

Der **bi-Cube[®] USB-Blocker** kann bei aktivierter NDS-Anbindung Gruppen und User auswerten, welche sich direkt unterhalb der Organisation und auch in OU's befinden. Daraus ergeben sich folgende Konstellationen bei den Mitgliedschaften:

1. Der User ist direkt unterhalb der Organisation angelegt.
 - a) Der User ist Mitglied einer Gruppe, welche ebenfalls direkt unterhalb der Organisation angelegt wurde.
 - b) Der User ist Mitglied einer Gruppe, welche sich in einer OU befindet.
2. Der User ist innerhalb einer OU angelegt worden.
 - a) Der User ist Mitglied einer Gruppe, welche ebenfalls direkt unterhalb der Organisation angelegt wurde.
 - b) Der User ist Mitglied einer Gruppe, welche sich in derselben OU befindet wie der des Users.
 - c) Der User ist Mitglied einer Gruppe, welche sich in einer anderen OU befindet, wie der des Users.

3.2.3.2 Konfigurationshinweise für die NDS-Nutzung

Es wird weiterhin empfohlen, dass der USB-Blocker Admin auf einem PC installiert wird, von dem aus Verwaltungszugriff (ConsoleOne, Webadministration) auf das NDS möglich ist. Die Gruppen für die Verwaltung der Geräte und User müssen von Hand im NDS angelegt werden.

Hinweis:

Für den im Punkt [3.2.2.4](#) beschriebenen administrativen Novell User wird empfohlen folgendes zu beachten: Damit der **bi-Cube[®] USB-Blocker** mit dem angegebenen User konkurrierende (gleichzeitige) Abfragen für Gruppen im NDS tätigen kann, sollten für diesen User keine Login Restrictions bestehen.

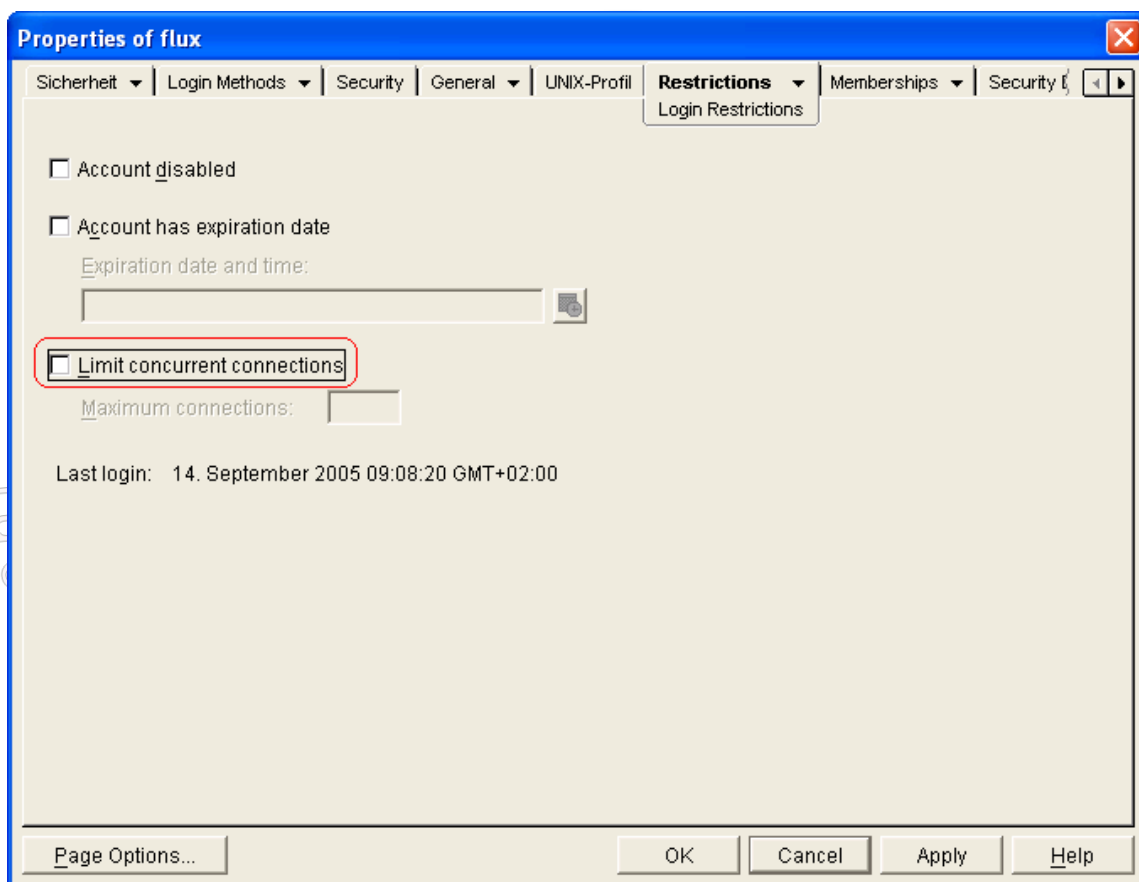


Abbildung 10 Einstellungen für den administrativen NDS-User

3.3 Installation per Softwareverteilung

Um die Installation in einem Netzwerk zu erleichtern, kann der **bi-Cube[®] USB-Blocker** über Systeme zur Softwareverteilung an die Client-Rechner verteilt werden.

Eine über die Softwareverteilung einer Windows 2000/2003 Domäne verteilungsfähige **MSI-Datei** sowie eine **MST-Datei** mit Ihren Lizenzdaten werden durch den Hersteller bereitgestellt. Die Installation der **InstallShield Skript-Engine 8** ist nur erforderlich, wenn die Installation auf den Clients mit einer entsprechenden Fehlermeldung im Anwendungsprotokoll fehlschlägt.

Die mit Hilfe des USB-Blocker Admin exportierte Konfigurationsdatei **usbblock.reg** (3.2.2.5) wird ebenfalls per Softwareverteilung an die Clients übermittelt. Dazu muss sich diese lediglich im gleichen Ordner wie das zu verteilende msi-Paket befinden. Sie wird dann automatisch bei der Installation verwendet.

3.4 Verwaltung des **bi-Cube[®] USB-Blockers** per Gruppenrichtlinien(GPO)

Nach der Installation der Admin-Oberfläche befindet sich im Installationsverzeichnis des **bi-Cube[®] USB-Blockers** eine **ADM-Datei**, die in eine **GPO** eingebunden werden kann. Auf diese Weise ist es möglich, die Konfiguration des **bi-Cube[®] USB-Blockers** auf den Clients komfortabel zu ändern.

Kopieren Sie dazu die ADM-Datei in das Verzeichnis C:\Windows\inf des Domänencontrollers. Öffnen Sie den **Gruppenrichtlinien-Editor** und erstellen Sie eine neue GPO.

Öffnen Sie die **GPO** und klicken Sie mit der rechten Maustaste in der Kategorie **Computerkonfiguration** auf **Administrative Vorlagen**, wählen **Vorlagen hinzufügen/Entfernen** und fügen das USB-Blocker-ADM als Vorlage hinzu.

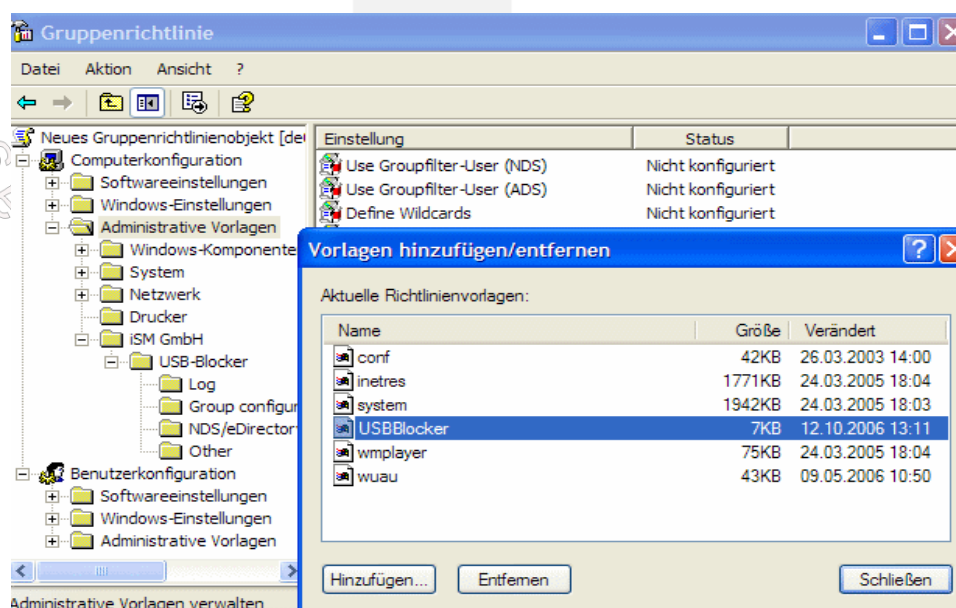


Abbildung 11 Gruppenrichtlinien-Editor

Da es sich bei den Richtlinieneinstellungen des **bi-Cube[®] USB-Blockers** um nicht vollständig verwaltbare Richtlinieneinstellungen handelt, muss die entsprechende Filterung deaktiviert werden. Das erreichen Sie indem Sie die Kategorie **Administrative Vorlagen** auswählen und unter **Ansicht** die Filterung deaktivieren.

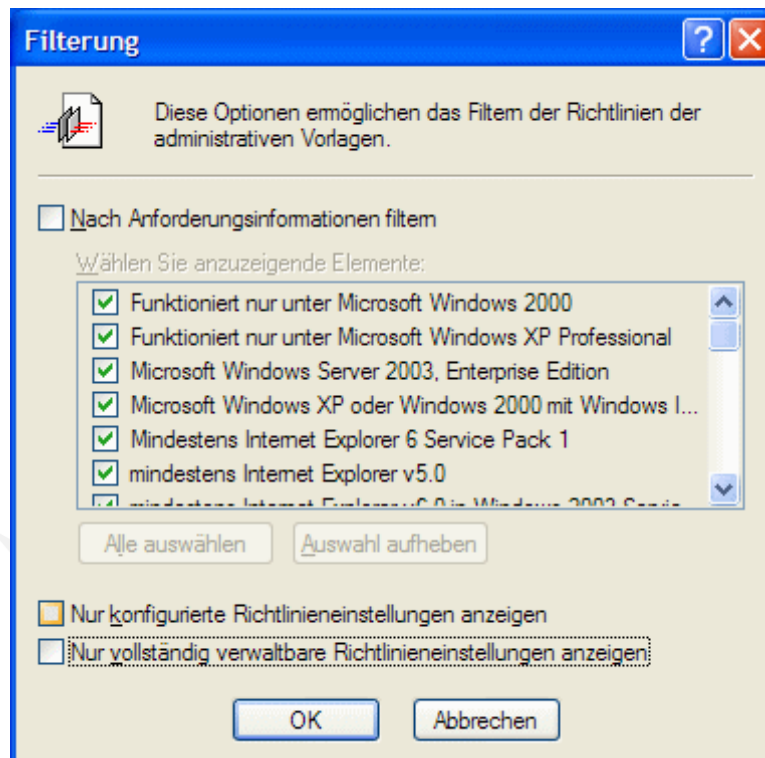


Abbildung 12 Filterung der Richtlinieneinstellungen

3.5 **bi-Cube[®] USB-Blocker 30-Tage-Testversion**

Während der Testphase von 30 Tagen können Sie den **bi-Cube[®] USB-Blocker** uneingeschränkt nutzen.

Bei jedem Start des Dienstes **USB-Blocker** wird für 120 Sekunden ein Infofenster eingeblendet. Dieses Infofenster können Sie jederzeit schließen. Auch beim Start des **USB-Blocker Admin** wird Ihnen das Infofenster eingeblendet. Schließen Sie dieses, indem Sie auf die Schaltfläche **Close** klicken.



Abbildung 13 Infofenster

Nach Ablauf dieser Testphase lässt sich der Dienst **USB-Blocker** nicht mehr starten. Beim Versuch, den Dienst zu starten, beendet der Dienst sich selbst. Über diesen Vorgang wird im System-Ereignisprotokoll informiert.

Ab diesem Zeitpunkt können alle Benutzer den Rechner wieder uneingeschränkt verwenden. Eine Überprüfung der Mitgliedschaft in den definierten Gruppen findet nicht mehr statt.

4 Ergebnisse - Beispielkonfiguration

Ziel der Beispielkonfiguration soll das Deaktivieren aller USB-Massenspeicher sein. USB-Geräte, die keine Massenspeicher sind, werden nach wie vor funktionieren. Zusätzlich soll ein spezieller USB-Stick für einen Benutzer freigegeben werden.

Bitte lassen Sie nicht erwähnte Einstellungen für die beispielhafte Konfiguration auf den Standardwerten.

Es wird vorausgesetzt, dass auf dem Testrechner der **USB-Blocker Admin** installiert und ein USB-Stick angesteckt und funktionsbereit ist. Ferner wird Schreibzugriff auf das **Active Directory** bzw. **eDirectory** benötigt.

Für die Durchführung der nachfolgenden Schritte erfordert der **USB-Blocker Admin** lokale Admin-Rechte.

4.1 Active Directory

Gehen Sie folgendermaßen vor:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer**.
2. Erstellen Sie eine neue OU z.B. mit dem Namen „USB-Blocker“.
3. Erstellen Sie in dieser OU einen neuen Benutzer z.B. `usbblocker`. Deaktivieren Sie die Kontooption **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** und aktivieren Sie die Option **Kennwort läuft nie ab**.

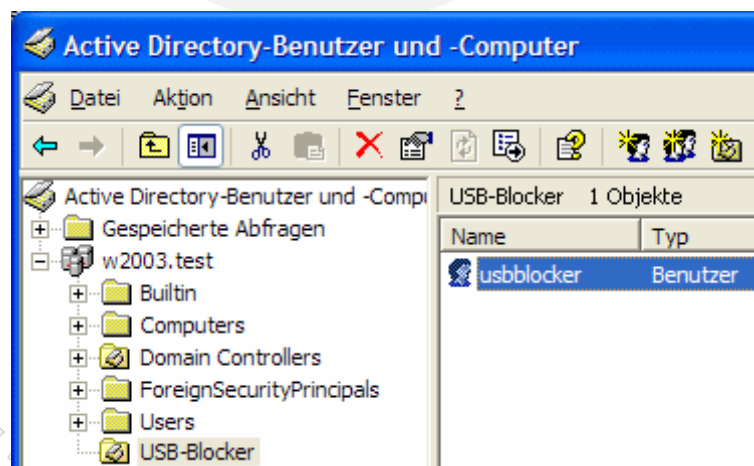


Abbildung 14 Erstellen AD-Benutzer

4. Lassen Sie die Konsole geöffnet und starten Sie den **USB-Blocker Admin** über das Startmenü.
5. Wechseln Sie über den Button **Konfiguration** in die Konfigurationsansicht.
6. Klicken Sie auf **Andere Konfigurationen**.
7. Aktivieren Sie die Option **Nutze Gruppenfilter Benutzer (ADS)**.
8. Tragen Sie in die Felder den zuvor angelegten Nutzer `usbblocker` und die Domäne ein.

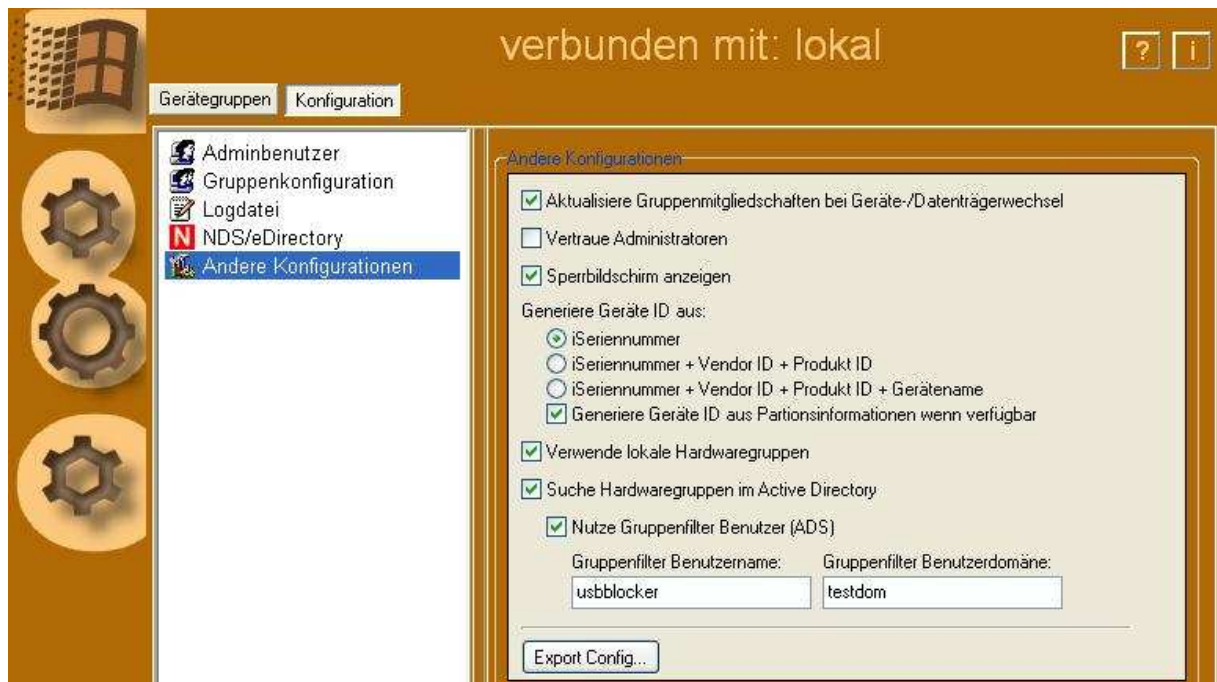


Abbildung 15 Gruppenfilter Benutzer (ADS) eintragen

9. Wechseln Sie über den Button **Gerätegruppen** in die Gerätebaum-Ansicht des **USB-Blocker Admins**.
10. Klicken Sie auf den Knoten **Laufwerke (Windows XP)** bzw. **Datenträger (Windows 2000)**.
11. Klicken Sie auf den USB-Stick, den Sie zur Benutzung freigeben möchten.
12. Kopieren Sie auf der rechten Seite **Gruppennamen für Geräteklasse: hw_cl_usbstor**. Dieser Gruppenname beschreibt alle Geräte der Klasse USB-Massenspeicher.

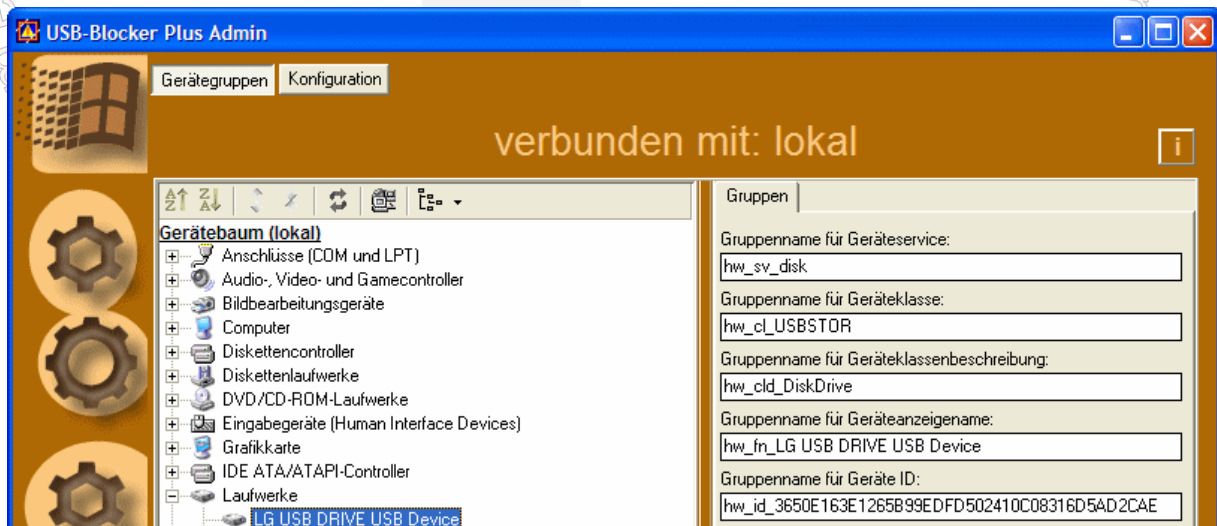


Abbildung 16 AD - Gruppenname für Geräteklasse eintragen

13. Wechseln Sie zurück zur Konsole **Active Directory-Benutzer und -Computer** und legen Sie eine Gruppe **hw_cl_usbstor** in der OU des **USB-Blockers** an. Es werden globale und universale Gruppen vom Typ Sicherheit unterstützt.

14. Wechseln Sie zum **USB-Blocker Admin** und kopieren Sie auf der rechten Seite **Gruppenname für Geräteanzeigename**, z.B. **hw_fn_LG USB DRIVE USB Device**. Dieser Gruppenname beschreibt nur das gerade angesteckte bzw. baugleiche Geräte.
15. Legen Sie auch diese Gruppe im AD an.
16. Machen Sie anschließend den zu Beginn erstellten Benutzer **usbblocker** zum Mitglied in beiden Gruppen.
17. Machen Sie einen Benutzer (z.B. Otto), der das Recht zur Nutzung des Gerätes bekommen soll, nur zum Mitglied der Gruppe **Gruppenname für Geräteanzeigename**.

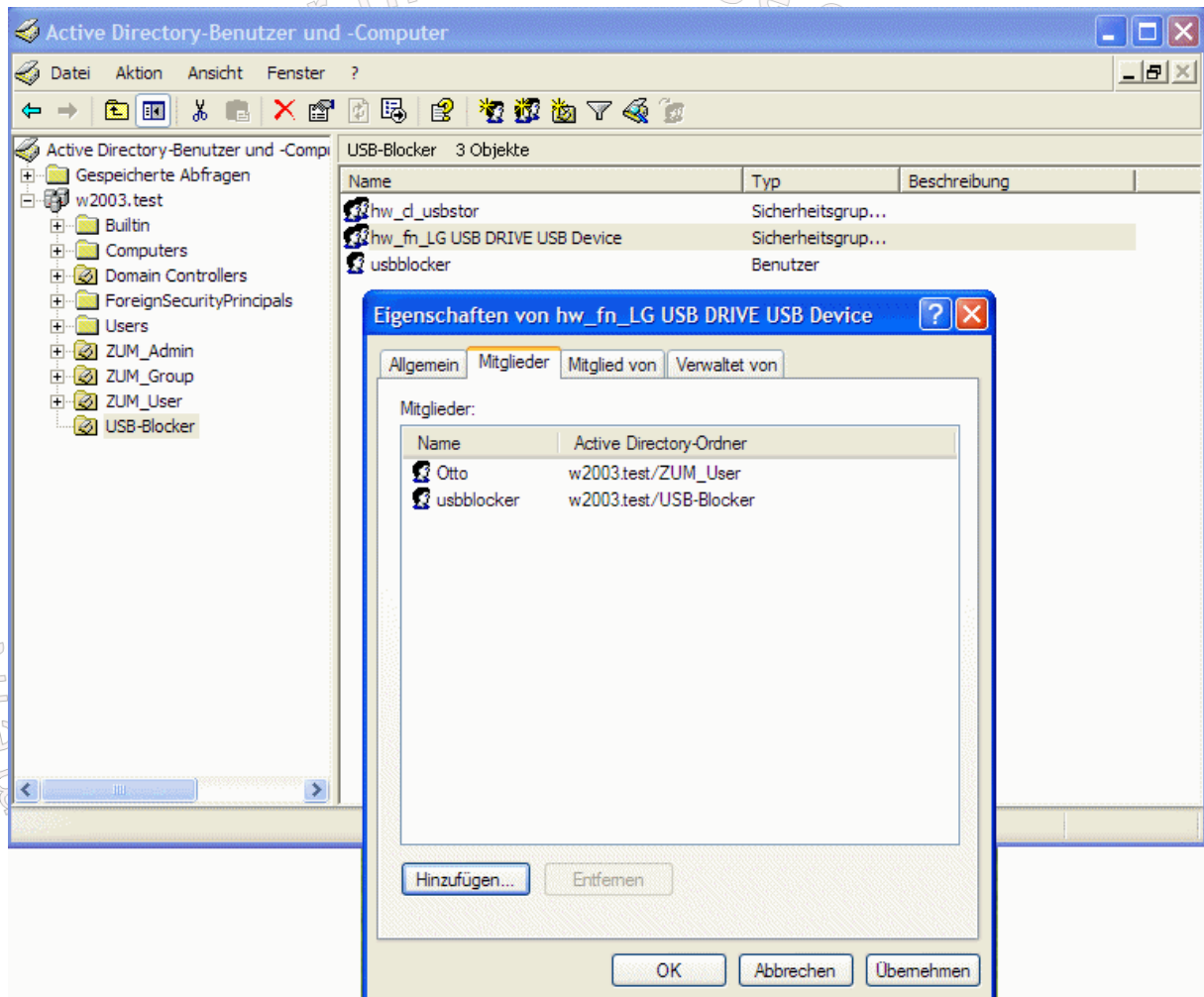


Abbildung 17 AD - Mitglied in Gruppenname für Anzeigename benennen

18. Starten Sie den Dienst **USB-Blocker** zum Einlesen der Berechtigungsdaten neu.

Ergebnis: Nach dem Neustart des Dienstes wird der Stick ausgeworfen, sofern es sich bei dem angemeldeten Nutzer nicht um ein Mitglied der Gruppe **Gruppenname für Geräteanzeigename** handelt.

Nach Anmeldung mit dem Nutzer Otto, der Mitglied in der Gruppe **Gruppenname für Geräteanzeigename** ist, kann der USB-Stick wieder verwendet werden. Dazu ist ein erneutes Anstecken des Gerätes nötig.

Begründung:

Es kommt im beschriebenen Fall eine restriktive Strategie zum Einsatz. Grundsätzlich werden alle USB-Massenspeicher geblockt. Dies geschieht aufgrund der Existenz der Gruppe **hw_cl_usbstor**. Die Mitgliedschaft eines Benutzers in einer Gruppe berechtigt zur Benutzung des entsprechenden Gerätes. Im Beispiel wurde „Otto“ Mitglied der Gruppe **Gruppenname für Geräteanzeigename**. Deshalb darf er das Gerät benutzen.

Grundsätzlich gilt:

1. Der **Gruppenfilter Benutzer** muss Mitglied in allen für den **bi-Cube[®] USB-Blocker** relevanten Gruppen sein. Dieser Account sollte für keine anderen Zwecke genutzt werden.
2. Die Mitgliedschaft in einer Gruppe berechtigt zur Benutzung der/des entsprechenden Geräte(s).

Hinweis:

Gruppenmitgliedschaften im AD werden erst nach einer Neuansmeldung wirksam.

Achtung: Wenn Sie den **bi-Cube[®] USB-Blocker** mit diesen Einstellungen auf einem anderen Rechner testen wollen, müssen Sie die Konfigurationseinstellungen übertragen. Exportieren Sie dazu die Konfiguration wie in Punkt [3.2.2.5h](#) beschrieben und führen Sie die reg-Datei auf dem Client-Rechner aus.

4.2 NDS/eDirectory

Gehen Sie folgendermaßen vor:

1. Öffnen Sie die **ConsoleOne** und verbinden Sie sich mit Ihrem Tree.
2. Erstellen Sie eine neue OU z.B. mit dem Namen „USB-Blocker“.
3. Erstellen Sie in dieser OU einen neuen Benutzer z.B. usbblocker.

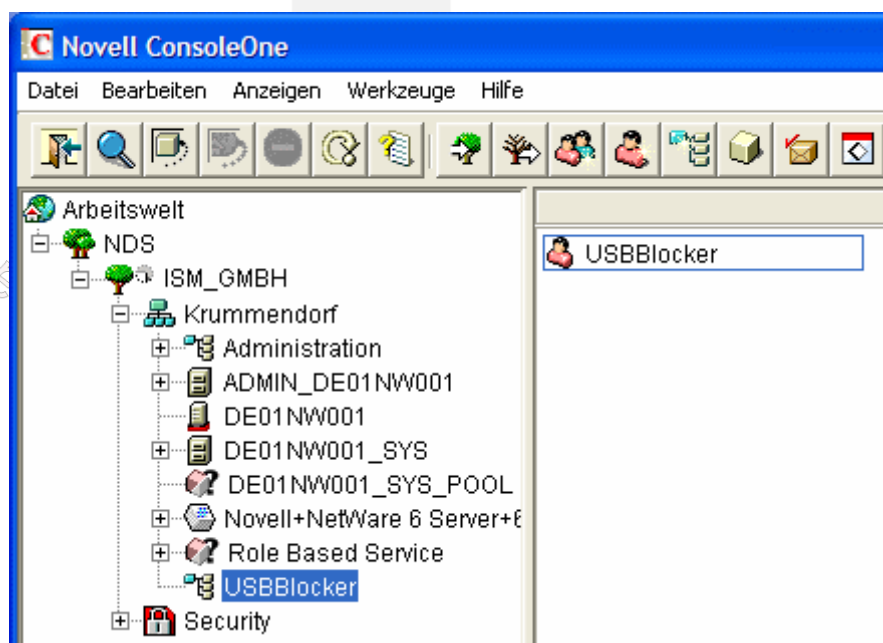


Abbildung 18 NDS – Neuen Benutzer in OU erstellen

4. Lassen Sie die **ConsoleOne** geöffnet und starten Sie den **USB-Blocker Admin** über das Startmenü.
5. Wechseln Sie über den Button **Konfiguration** in die Konfigurationsansicht.
6. Klicken Sie auf **NDS/eDirectory** und aktivieren Sie die Option **Benutze NDS/eDirectory**.

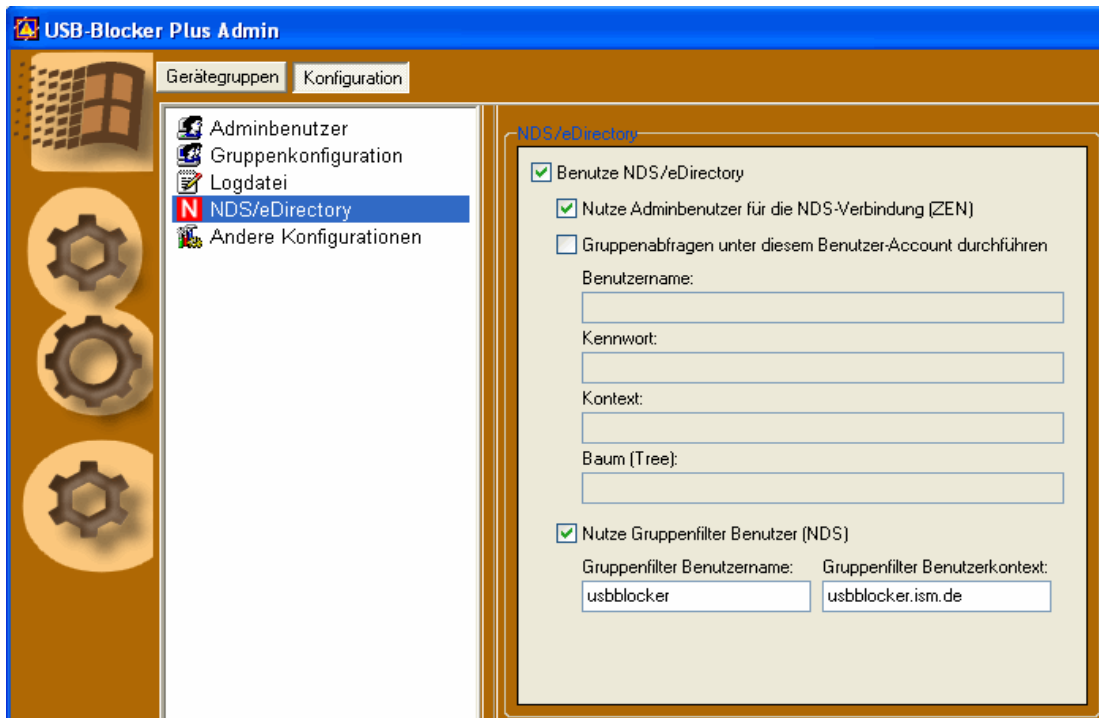


Abbildung 19 Konfiguration NDS/eDirectory

7. Aktivieren Sie die Option **Nutze Gruppenfilter Benutzer (NDS)**.
8. Tragen Sie in die Felder den zuvor angelegten Nutzer „usbblocker“ und seinen Kontext ein (ohne Tree!).
9. Wechseln Sie über den Button **Gerätegruppen** in die Gerätebaum-Ansicht des **USB-Blocker Admins**.
10. Klicken Sie auf den Knoten **Laufwerke (Windows XP)** bzw. **Datenträger (Windows 2000)**.
11. Klicken Sie auf den USB-Stick.
12. Kopieren Sie auf der rechten Seite **Gruppennamen für Geräteklasse: hw_cl_usbstor**. Dieser Gruppenname beschreibt alle Geräte der Klasse USB-Massenspeicher.

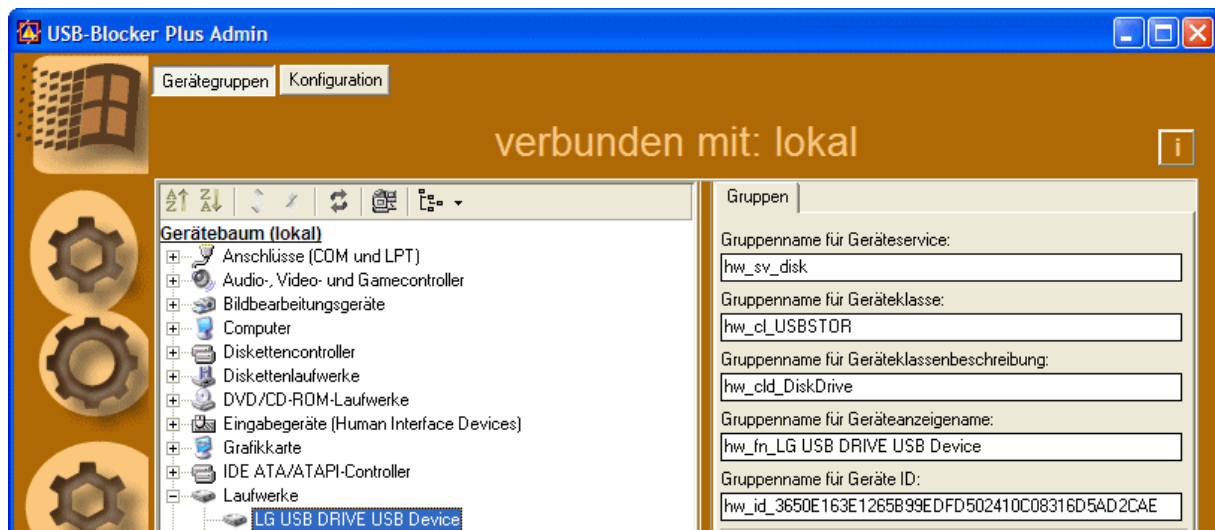


Abbildung 20 NDS - Gruppenname für Geräteklasse festlegen

13. Wechseln Sie zur **ConsoleOne** und legen Sie eine Gruppe **hw_cl_usbstor** in der OU des USB-Blockers an.
14. Wechseln Sie zum **USB-Blocker Admin** und kopieren Sie auf der rechten Seite **Gruppenname für Geräteanzeigename**, z.B. **hw_fn_LG USB DRIVE USB Device**. Dieser Gruppenname beschreibt nur das gerade angesteckte bzw. baugleiche Geräte.
15. Legen Sie auch diese Gruppe im **NDS/eDirectory** an.
16. Machen Sie anschließend den zu Beginn erstellten Benutzer „usbblocker“ zum Mitglied in beiden Gruppen.
17. Machen Sie einen beliebigen Benutzer (z.B. Otto), der das Recht zur Nutzung des Gerätes bekommen soll, nur zum Mitglied der Gruppe **Gruppenname für Geräteanzeigename**.

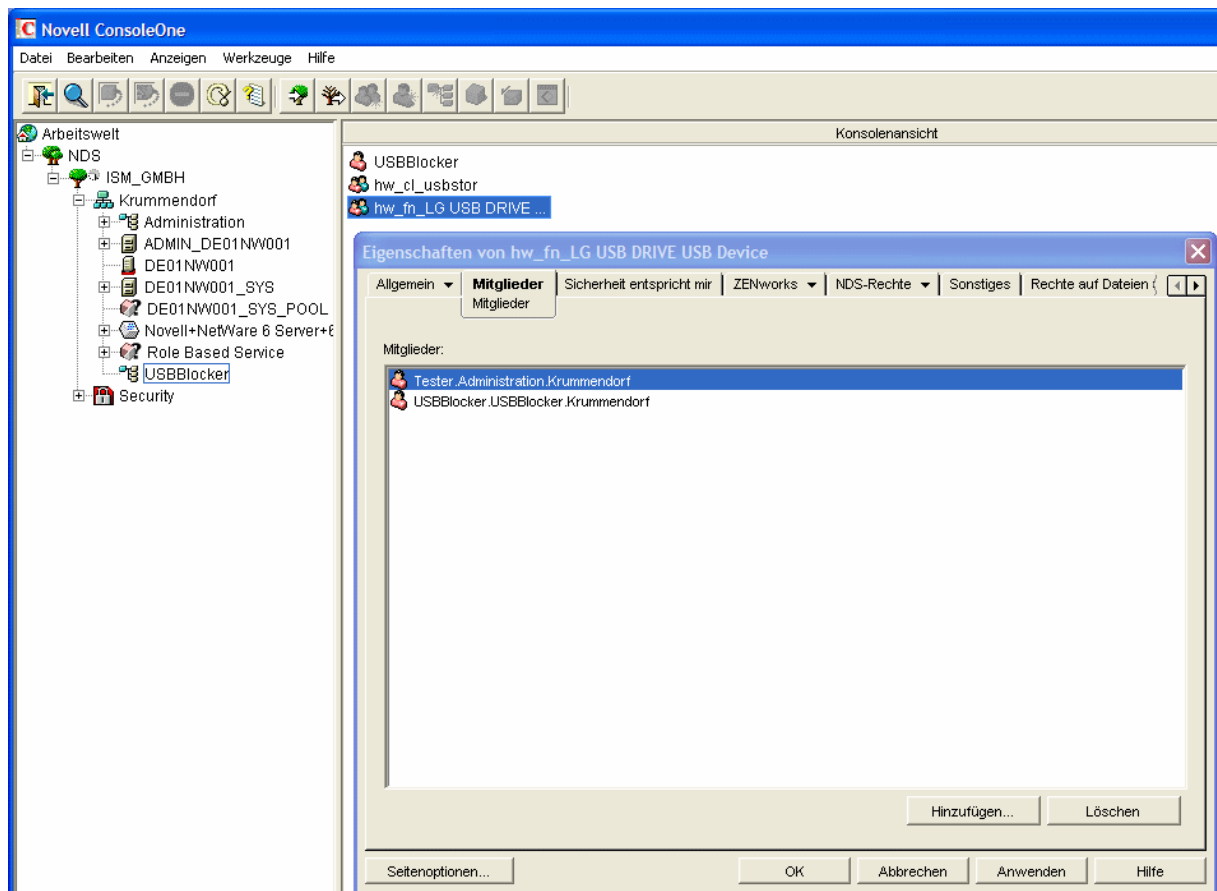


Abbildung 21 NDS - Mitglied in Gruppenname für Geräteanzeigename festlegen

18. Starten Sie den Dienst **USB-Blocker** zum Einlesen der Berechtigungsdaten neu.

Ergebnis: Nach dem Neustart des Dienstes wird der Stick ausgeworfen, sofern es sich bei dem angemeldeten Novell-Nutzer nicht um ein Mitglied der Gruppe **Gruppenname für Geräteanzeigename** handelt.

Nach Anmeldung mit dem Nutzer Otto, der Mitglied in der Gruppe **Gruppenname für Geräteanzeigename** ist, kann der USB-Stick wieder verwendet werden. Dazu ist ein erneutes Anstecken des Gerätes nötig.

Begründung:

Es kommt im beschriebenen Fall eine restriktive Strategie zum Einsatz. Grundsätzlich werden alle USB-Massenspeicher geblockt. Dies geschieht aufgrund der Existenz der Gruppe hw_cl_usbstor. Die Mitgliedschaft eines Benutzers in einer Gruppe berechtigt zur Benutzung des entsprechenden Gerätes. Im Beispiel wurde Tester Mitglied der Gruppe **Gruppenname für Geräteanzeigename**. Deshalb darf er das Gerät benutzen.

Grundsätzlich gilt:

1. Der Gruppenfilter Benutzer muss Mitglied in allen für den **bi-Cube[®] USB-Blocker** relevanten Gruppen sein. Dieser Account sollte für keine anderen Zwecke genutzt werden.
2. Die Mitgliedschaft in einer Gruppe berechtigt zur Benutzung der/des entsprechenden Geräte(s).

Achtung: Wenn Sie den **bi-Cube[®] USB-Blocker** mit diesen Einstellungen auf einem anderen Rechner testen wollen, müssen Sie die Konfigurationseinstellungen übertragen. Exportieren Sie dazu die Konfiguration wie in Punkt [3.2.2.5h](#) beschrieben und führen Sie die reg-Datei auf dem Client-Rechner aus.

4.3 Lokal

Gehen Sie folgendermaßen vor:

1. Öffnen Sie den **USB-Blocker Admin** über das Startmenü.
2. Aktivieren Sie unter **Konfiguration** → **Andere Konfigurationen** die Option **Verwende lokale Hardwaregruppen**
3. Zurück im Gerätebaum klicken Sie auf den **Knoten Laufwerke (Windows XP)** bzw. **Datenträger (Windows 2000)**.
4. Klicken Sie auf den USB-Stick.
5. Kopieren Sie auf der rechten Seite **Gruppennamen für Geräteklasse: hw_cl_usbstor**. Dieser Gruppenname beschreibt alle Geräte der Klasse USB-Massenspeicher.

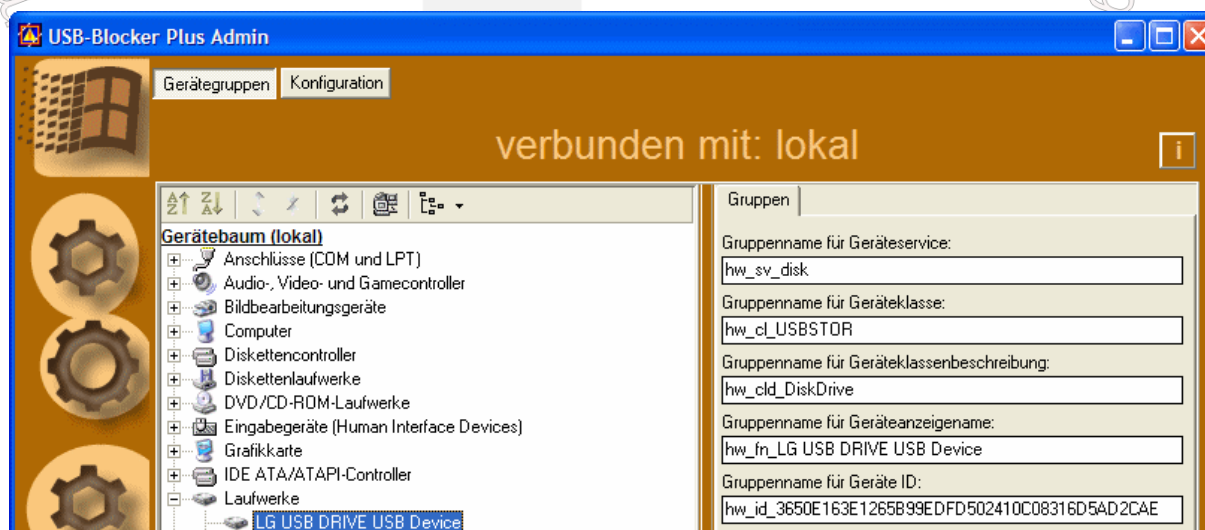


Abbildung 22 Lokal – Gruppenname für Geräteklasse festlegen

- Öffnen Sie die lokale Computerverwaltung und legen Sie eine Gruppe hw_cl_usbstor an.
- Wechseln Sie zum **USB-Blocker Admin** und kopieren Sie auf der rechten Seite **Gruppenname für Geräteanzeigename**, z.B. hw_fn_LG USB DRIVE USB Device. Dieser Gruppenname beschreibt nur das gerade angesteckte bzw. baugleiche Geräte.
- Legen Sie auch diese Gruppe mit der Computerverwaltungskonsole lokal an.
- Machen Sie einen Benutzer (z.B. Otto), der das Recht zur Nutzung des Gerätes bekommen soll, nur zum Mitglied der Gruppe **Gruppenname für Geräteanzeigename**.

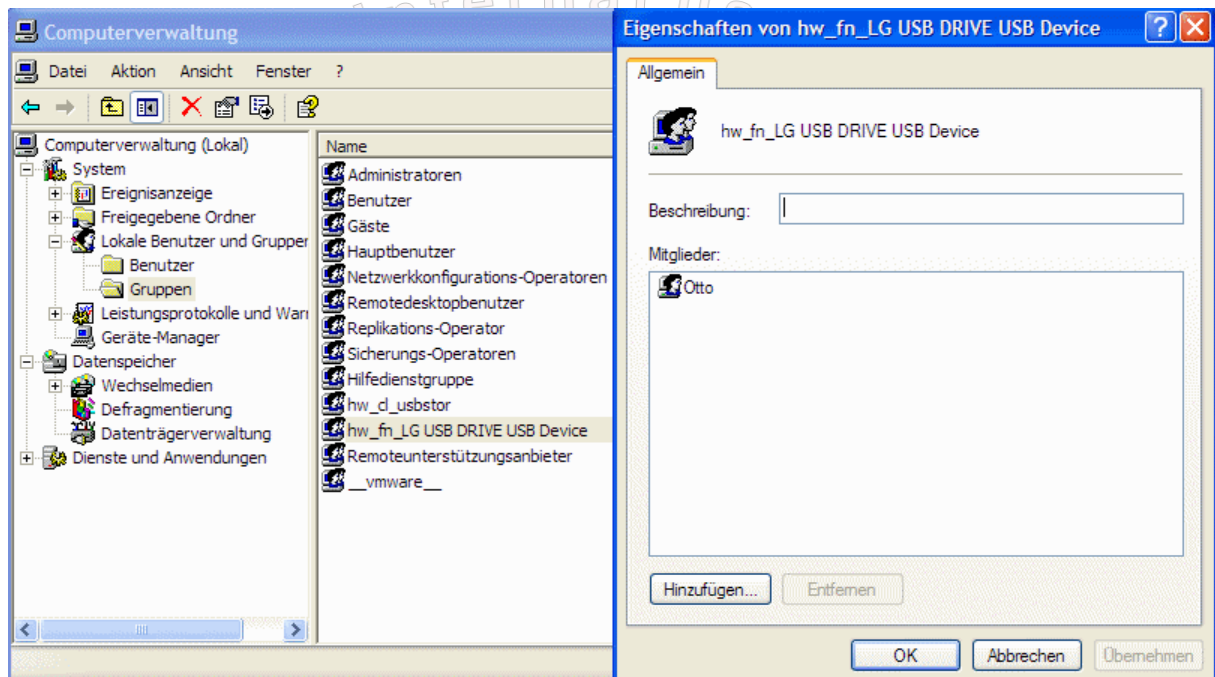


Abbildung 23 Lokal - Mitglied in Gruppenname für Geräteanzeigename festlegen

- Starten Sie den Dienst **USB-Blocker** zum Einlesen der Berechtigungsdaten neu.

Ergebnis: Nach dem Neustart des Dienstes wird der Stick ausgeworfen, sofern es sich bei dem angemeldeten Nutzer nicht um ein Mitglied der Gruppe **Gruppenname für Geräteanzeigename** handelt.

Nach Anmeldung mit dem Nutzer Otto, der Mitglied in der Gruppe **Gruppenname für Geräteanzeigename** ist, kann der USB-Stick wieder verwendet werden. Dazu ist ein erneutes Anstecken des Gerätes nötig.

Begründung:

Es kommt im beschriebenen Fall eine restriktive Strategie zum Einsatz: Grundsätzlich werden alle USB-Massenspeicher geblockt. Dies geschieht aufgrund der Existenz der Gruppe hw_cl_usbstor. Die Mitgliedschaft eines Benutzers in einer Gruppe berechtigt zur Benutzung des entsprechenden Gerätes. Im Beispiel wurde „Otto“ Mitglied der Gruppe **Gruppenname für Geräteanzeigename**. Deshalb darf er das Gerät benutzen.

Grundsätzlich gilt:

Die Mitgliedschaft in einer Gruppe berechtigt zur Benutzung der/des entsprechenden Geräte(s).

4.4 Sämtliche USB-Geräte deaktivieren

Um alle USB-Geräte zu deaktivieren, gibt es zwei Möglichkeiten:

4.4.1 Deaktivieren aller USB-Geräteklassen

Folgende Gruppen müssen existieren:

hw_cl_USBSTOR	- Sperrt alle USB-Massenspeicher, Kameras
hw_sv_USBPRINT	- Sperrt alle USB-Drucker
hw_cl_HID	- Sperrt alle USB-Human-Interface-Devices (Mäuse, Tastaturen)
hw_cld_Image	- Sperrt Scanner, Sensoren, Kameras
hw_sv_vmusb	- Sperrt die Übergabe von USB-Geräten an virtuelle VMware Guests
hw_cld_cl_USB_Net	- Sperrt USB-Netzwerkadapter
hw_cld_cl_USB_Bt	- Sperrt USB-Bluetooth-Devices

Anschließend können die gerätebezogenen Gruppen angelegt werden, um die Verwendung bestimmter Geräte zu erlauben.

Dies ist die empfohlene Vorgehensweise.

4.4.2 Deaktivieren des USB-Hubs

Folgende Gruppe muss existieren:

hw_cl_USB	- Sperrt den USB-Hub
------------------	----------------------

Ein User, dem es erlaubt ist ein USB-Gerät zu nutzen, muss auch Mitglied in dieser Gruppe sein. Grund hierfür ist, dass der Computer die Änderung der Gerätekonfiguration nicht erkennt, wenn der USB-Hub deaktiviert ist.

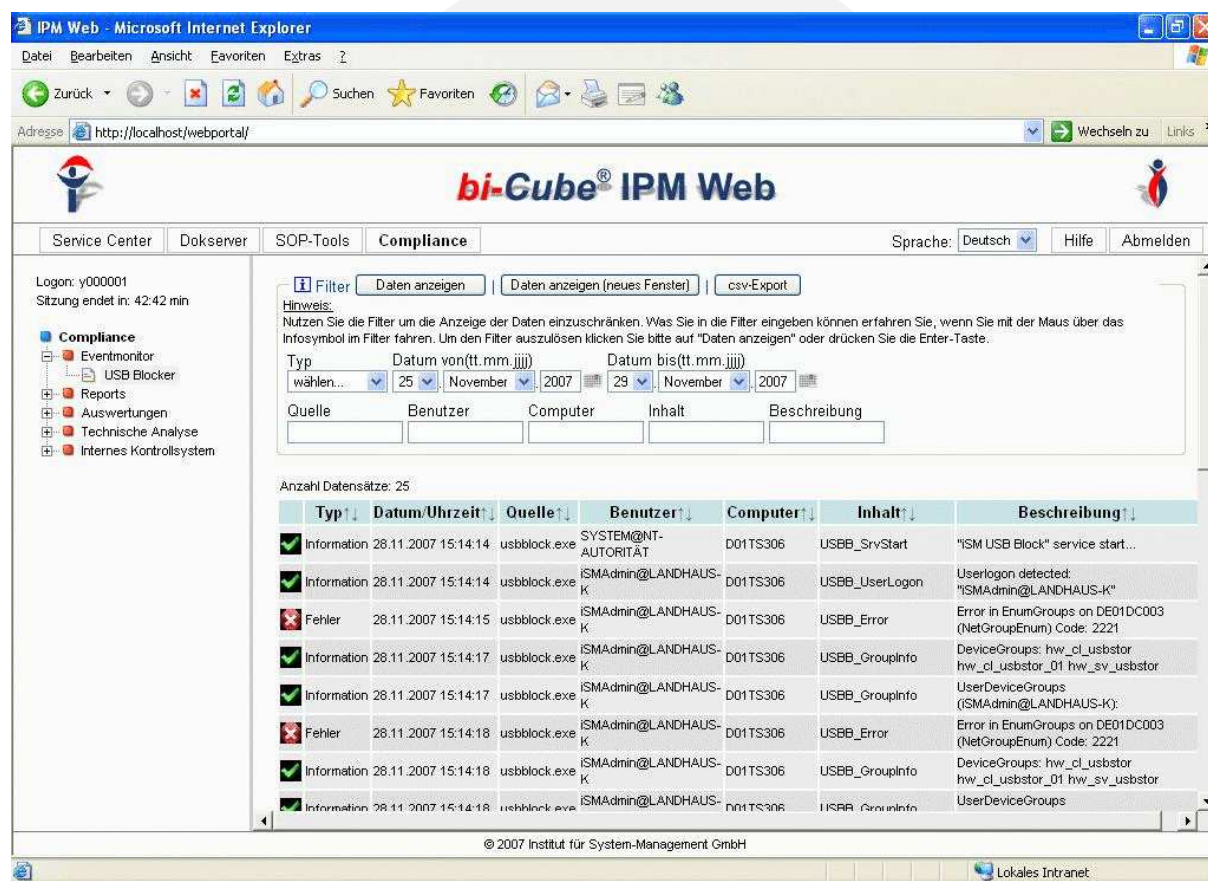
Diese Vorgehensweise empfiehlt sich, wenn USB-Geräte nie verwendet werden.

5 Erweiterung der Funktionen des **bi-Cube[®] USB-Blocker** mit **bi-Cube[®] IPM**

Die Funktionen des **bi-Cube[®] USB-Blocker** können durch die Verwendung von **bi-Cube[®] IPM** sinnvoll erweitert werden.

bi-Cube[®] IPM ermöglicht eine automatisierte, zentrale Steuerung und Verwaltung des **bi-Cube[®] USB-Blocker**. Das automatische Anlegen der Gerätegruppen im **AD**, ein Rollenmodell mit umfassenden Modellierungsmöglichkeiten und Monitoring per Weboberfläche sind nur einige der vielen Erleichterungen, die **bi-Cube[®] IPM** dem Systemverwalter bietet.

Dank des **bi-Cube[®]** Baukastensystems kann für Sie eine sehr individuelle Lösung zusammengestellt werden.



IPM Web - Microsoft Internet Explorer

Adresse: http://localhost/webportal/

bi-Cube[®] IPM Web

Service Center | Dokserver | SOP-Tools | **Compliance** | Sprache: Deutsch | Hilfe | Abmelden

Logon: y000001
Sitzung endet in: 42:42 min

Compliance

- Eventmonitor
- USB Blocker
- Reports
- Auswertungen
- Technische Analyse
- Internes Kontrollsystem

Hinweis:
Nutzen Sie die Filter um die Anzeige der Daten einzuschränken. Was Sie in die Filter eingeben können erfahren Sie, wenn Sie mit der Maus über das Infosymbol im Filter fahren. Um den Filter auszulösen klicken Sie bitte auf "Daten anzeigen" oder drücken Sie die Enter-Taste.

Filter:
 Typ: wählen... Datum von (tt.mm.jjjj): 25. November 2007 Datum bis (tt.mm.jjjj): 29. November 2007
 csv-Export

Typ	Datum/Uhrzeit	Quelle	Benutzer	Computer	Inhalt	Beschreibung
Information	28.11.2007 15:14:14	usbblock.exe	SYSTEM@NT-AUTORITÄT	D01TS306	USBB_SrvStart	"ISM USB Block" service start...
Information	28.11.2007 15:14:14	usbblock.exe	ISMAdmin@LANDHAUS-K	D01TS306	USBB_UserLogon	Userlogon detected: "ISMAdmin@LANDHAUS-K"
Fehler	28.11.2007 15:14:15	usbblock.exe	ISMAdmin@LANDHAUS-K	D01TS306	USBB_Error	Error in EnumGroups on DE01DC003 (NetGroupEnum) Code: 2221
Information	28.11.2007 15:14:17	usbblock.exe	ISMAdmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	DeviceGroups: hw_cl_usbstor hw_cl_usbstor_01 hw_sv_usbstor
Information	28.11.2007 15:14:17	usbblock.exe	ISMAdmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	UserDeviceGroups (ISMAdmin@LANDHAUS-K):
Fehler	28.11.2007 15:14:18	usbblock.exe	ISMAdmin@LANDHAUS-K	D01TS306	USBB_Error	Error in EnumGroups on DE01DC003 (NetGroupEnum) Code: 2221
Information	28.11.2007 15:14:18	usbblock.exe	ISMAdmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	DeviceGroups: hw_cl_usbstor hw_cl_usbstor_01 hw_sv_usbstor
Information	28.11.2007 15:14:18	usbblock.exe	ISMAdmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	UserDeviceGroups

© 2007 Institut für System-Management GmbH

Lokales Intranet

Abbildung 24 Zentrales Monitoring des USB-Blockers

6 Hinweise

- Testen Sie in jedem Fall, ob die beabsichtigte Wirkung erreicht wird und keine unbeabsichtigten Wechselwirkungen (durch übergreifende Gruppen bzw. Verbundgeräte) entstehen.
- Es kann nicht garantiert werden, dass die Verwendung der ermittelten Gruppen immer zum selben Ergebnis führt.

7 FAQ

1. **Welcher Gruppenbereich und Gruppentyp soll für Gruppen im AD verwendet werden?**
 - a. Es werden globale und universelle Gruppen vom Typ Sicherheit unterstützt. Dies entspricht den Hinweisen von Microsoft bzgl. des Gruppendesigns im Active Directory.
2. **Welche Kontooptionen müssen am Gruppenfilter-User aktiviert sein?**
 - a. Bitte stellen Sie sicher, dass der User das Passwort bei der ersten Anmeldung nicht ändern muss und das Passwort nie abläuft.
3. **Wie muss die .mst-Datei bei der Verteilung angewendet werden, damit der **bi-Cube[®] USB-Blocker** mit den Lizenzdaten auf den Clients installiert wird?**
 - a. Um eine unbeaufsichtigte Installation durchzuführen und die .mst-Datei mit den Lizenzdaten auf das msi-Paket anzuwenden, muss folgender Befehl ausgeführt werden:
„USB-Blocker Plus.msi TRANSFORMS=.mst-Datei /qb“
4. **Der Blockbildschirm verschwindet nach kurzer Zeit?**
 - a. Dies ist das beabsichtigte Verhalten. Der **bi-Cube[®] USB-Blocker** sperrt nur so lange die Arbeitsstation wie benötigt wird, um alle zu sperrenden Geräte aus dem System zu entfernen.
Die Eingabefelder am rechten unteren Bildschirmrand werden in der Regel nicht benötigt. Durch die Eingabe eines Administrator-Accounts kann der Bildschirm entsperrt werden, wenn ein Gerät nicht ausgeworfen werden kann.
5. **Wie steht es um die die Sicherheit im abgesicherten Modus?**
 - a. Der abgesicherte Modus nimmt es (obwohl der Name Gegenteiliges vermuten lässt) mit der Sicherheit im Sinne des **bi-Cube[®] USB-Blockers** nicht sehr genau. In diesem Modus werden nur wenige Systemtreiber und Dienste geladen. Der **bi-Cube[®] USB-Blocker** gehört nicht dazu. Demzufolge ist es theoretisch möglich über den abgesicherten Modus Dateien ein- bzw. auszuschleusen. Dieses Problem betrifft in abgewandelter Form z.B. auch Virens Scanner oder Firewalls. Der einzig wirkungsvolle Ansatz liegt im Deaktivieren der Netzwerkfunktionalität des abgesicherten Modus, um eine Anmeldung mit einem Domänen-Account zu verhindern (unter der Annahme, dass den Usern keine lokalen Accounts bekannt sind).
Zu erreichen ist dies durch das Umbenennen des Schlüssels
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
in z.B.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Networkfals
e.
6. **Ich habe einen Domänen-Benutzer zum Mitglied einer Sperrgruppe gemacht. Warum kann das freigegebene Gerät trotzdem nicht genutzt werden?**
 - a. Änderungen von Gruppenmitgliedschaften werden in einer Windows-Domäne erst nach einer Neuanmeldung aktiv.

Abbildungsverzeichnis

Abbildung 1 USB-Blocker Admin	10
Abbildung 2 Gerätedetailanzeige	11
Abbildung 3 Geräte nach Verbindung	12
Abbildung 4 Umschalten der Programmansichten.....	15
Abbildung 5 Einstellungen für den USB-Blocker Admin User.....	16
Abbildung 6 Einstellungen für die Gruppenkonfiguration.....	16
Abbildung 7 Einstellungen für die Log-Tätigkeit.....	17
Abbildung 8 Einstellungen für die NDS/eDirectory Unterstützung.....	18
Abbildung 9 Einstellungen der Zusatzparameter	20
Abbildung 10 Einstellungen für den administrativen NDS-User.....	21
Abbildung 11 Gruppenrichtlinien-Editor	22
Abbildung 12 Filterung der Richtlinieneinstellungen	23
Abbildung 13 Infofenster	24
Abbildung 14 Erstellen AD-Benutzer.....	25
Abbildung 15 Gruppenfilter Benutzer (ADS) eintragen	26
Abbildung 16 AD - Gruppenname für Geräteklasse eintragen	26
Abbildung 17 AD - Mitglied in Gruppenname für Anzeigenamen benennen	27
Abbildung 18 NDS – Neuen Benutzer in OU erstellen.....	28
Abbildung 19 Konfiguration NDS/eDirectory	29
Abbildung 20 NDS - Gruppenname für Geräteklasse festlegen	30
Abbildung 21 NDS - Mitglied in Gruppenname für Geräteanzeigenamen festlegen	31
Abbildung 22 Lokal – Gruppenname für Geräteklasse festlegen	32
Abbildung 23 Lokal - Mitglied in Gruppenname für Geräteanzeigenamen festlegen	33
Abbildung 24 Zentrales Monitoring des USB-Blockers	35