

bi-Cube[®] Guideline

bi-Cube[®] USB-Blocker

Technologies Solutions Trends Experience



Contents

1	Objective	4
2	Requirements and Solution	4
2.1	How does the <i>bi-Cube[®]</i> USB-Blocker work?.....	5
2.2	How secure is the <i>bi-Cube[®]</i> USB-Blocker?.....	6
3	Implementation	7
3.1	Program Installation	7
3.1.1	System Requirements.....	7
3.1.2	Installing the <i>bi-Cube[®]</i> USB-Blocker.....	7
3.1.3	Uninstalling the <i>bi-Cube[®]</i> USB-Blocker.....	8
3.2	Operating the Program	8
3.2.1	Creating Groups.....	9
3.2.1.1	Preliminary considerations.....	9
3.2.1.2	Determine group names.....	10
3.2.1.3	Restrict writing rights.....	12
3.2.1.4	Naming conventions.....	13
3.2.1.5	Manage memberships.....	13
3.2.1.5.1	How to set up a local group.....	13
3.2.1.5.2	How to delete a local group.....	14
3.2.1.5.3	How to add a member to a group.....	14
3.2.1.5.4	How to delete a member from a group.....	14
3.2.1.6	Windows XP Home Edition.....	15
3.2.2	Configuring the <i>bi-Cube[®]</i> USB-Blocker.....	15
3.2.2.1	<i>bi-Cube[®]</i> USB-Blocker Admin user.....	15
3.2.2.2	Settings for group configuration.....	16
3.2.2.3	Settings for the <i>bi-Cube[®]</i> USB-Blocker log activity.....	17
3.2.2.4	Settings for NDS support.....	18
3.2.2.5	Settings for additional parameters.....	19
3.2.3	Group administration in NDS.....	20
3.2.3.1	Possible group constellations.....	20
3.2.3.2	Configuration hints for the NDS usage.....	20
3.3	Installation via software distribution	21
3.4	Administration of <i>bi-Cube[®]</i> USB-Blockers via Group Policies (GPO)	22
3.5	<i>bi-Cube[®]</i> USB-Blocker 30 Days Trial Version	24
4	Results - Example of configuration	25
4.1	Active Directory.....	25
4.2	NDS/eDirectory.....	28
4.3	Locally.....	32
4.4	Deactivate all USB devices.....	34
4.4.1	Disable all USB device classifications.....	34
4.4.2	Disable the USB hub.....	34
5	Extension of the <i>bi-Cube[®]</i> USB-Blocker functions with <i>bi-Cube[®]</i> IPM	35

6	Notes	36
7	FAQ	36
	Directory – Pictures	37

for internal use only



copyright by ISM-Institut für System-Management

1 Objective

How can the following be achieved with **bi-Cube[®]** ...

- That in the company the usage of almost any hardware can be controlled?

2 Requirements and Solution

USB devices become more and more wide-spread which also adds to new requirements against the administration. Particularly, the small USB flash drives introduce new dimensions. Not only their handling is quite easy, they are perfectly suitable for mobile saving of sensitive data, but also enable fast and almost unseen data thefts.

In the past, various measures have been implemented to secure a computer by switching off or removing a CD-ROM and floppy drives. But these 'simple' (hardware) security measures cannot be used with USB flash drives. The difference between various USB devices, e.g. printers, hubs or USB flash drives cannot be distinguished.

The **bi-Cube[®] USB-Blocker** Version 1.0 made it possible to control the use of USB mass storage according to defined user rights.

With today's **bi-Cube[®] USB-Blocker** many new and extensive options to control the use of almost any hardware in your company is available.

2.1 How does the **bi-Cube[®]** USB-Blocker work?

The function of the **bi-Cube[®]** USB-Blocker is very simple.

Every device in your computer includes diverse properties. A list of these properties can be displayed in the Windows Device Manger.

1. To open the Device Manager, click on **Start**, then on **System control**. Double click on **System**. In the tab **Hardware**, click on **Device Manager**.
2. Choose a hardware device from the tree structure, e.g. a DVD/CD-ROM drive of your computer.
3. In the menu item **Action**, click **Properties**. Now the properties of the device are displayed.
4. In tab **Details** a selection of the properties are shown.

Some of these properties identify the device itself, others describe the affiliation to various classes, services etc.

The classification and service affiliation of single devices or as a group can be monitored by the **bi-Cube[®]** USB-Blocker.

Should a device, a device group, or a service etc. be monitored by the **bi-Cube[®]** USB-Blocker, it is required to have an existing group with the same name on the computer or in the network. Access to this device is granted only to members of this group.

Therewith it also controls the user access to internal devices e.g. CD-ROM or disk drive.

The **bi-Cube[®]** USB-Blocker supports the directory services **Active Directory** and **Novell eDirectory (NDS)**. Necessary connections are only established as needed.

The program is installed on every workstation to be controlled and it is set up as a Windows service. It is launched automatically via the Windows operating system.

Note:

The USB-Blocker service grants the controlling of devices. During the installation the program is set up so that only administrators can end it.

With the logon of the user, the **bi-Cube[®]** USB-Blocker is activated:

- It determines the groups which already exist locally or in the network, as well as the groups to which the logged on user is a member of.
- It additionally stores the information as files.
- It controls if the devices, which are connected to and installed on the workstations, should be monitored and if the user is authorized to use them.
- It locks the user's screen (optionally) until the unauthorized device is removed or the locking is disabled by an administrator.

2.2 How secure is the **bi-Cube[®]** USB-Blocker?

All components required for the **bi-Cube[®]** USB-Blocker are visible for the standard user, but not changeable. The services "iSM USBBlockService" and "iSM Drive Protect", the user "USBAdmin" as well as the files in the installation folder are included in these components.

We generally advise against assigning administrator rights to the user. These rights include a number of options to deactivate or evade software. A standard user has no possibility to bypass the monitoring function of the **bi-Cube[®] USB-Blocker.**

The local user **USBAdmin** is used to eject or disable prohibited hardware. This user will be created during the installation and is a member of the administrator's group. To avoid misuse, for every installation a new random password is assigned to the USBAdmin.



3 Implementation

3.1 Program Installation

3.1.1 System Requirements

The **bi-Cube[®] USB-Blocker** can be installed to the following operating systems:

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

On 64bit operating systems the basic function like locking or blocking of devices is supported. At this time, not yet the write-protect function.

For the administration of groups the following systems can be used:

- Active Directory
- Novell eDirectory (NDS)
- local Windows groups

In general: 20 MB of free disc space is required during the installation.

Note: Windows NT is not supported!

bi-Cube[®] USB-Blocker cannot be installed to a domain controller

3.1.2 Installing the **bi-Cube[®] USB-Blocker**

The download package includes the files **USB-Blocker PLUS.exe**, **USB-Blocker PLUS.msi** and **isscript8.msi**. The MSI packages serve for the software distribution (3.3). The InstallShield script engine must only be distributed in case the installation causes an error in the application protocol of the target system, due to the USB-Blocker PLUS.msi package.

The **bi-Cube[®] USB-Blocker works without server component. The installation on a server is not necessary. The installation of the configuration interface to an administrator workstation is sufficient.**

To install the **bi-Cube[®] USB-Blocker**, please start the **USB-Blocker PLUS.exe**, choose the setup language and follow the instructions!

If required during setup, please enter the license number into the appropriate fields. You can find your license number in the information sheet which you have received by the Institut für System-Management GmbH via e-mail or postal service. For testing purposes you may also install the program as a 30 day trial version.

For the **bi-Cube[®] USB-Blocker** configuration, the **USB-Blocker Admin** program is available for you. To install it, please choose the appropriate option.

The **bi-Cube[®] USB-Blockers** Setup:

- copies the needed files on the computer,
- installs and launches the services “iSM USBBlockService” and “iSM Drive Protect“,
- generates a local user USBAdmin with a random password and equips him with local administrator rights and
- creates the program group USB-Blocker in the Start menu and some menu entries.

Note:

The Services “iSM USBBlockService” and “iSM Drive Protect“ are launched when the installation is completed. If there are already existing groups for monitoring on the computer or in the network (domain), the Access Control is activated immediately.

3.1.3 Uninstalling the **bi-Cube[®] USB-Blocker**

The program can be uninstalled by using the Windows service program software.

1. Click on **Start** to open the service program software, click on **System control** and then click on **Software**.
2. From the list of installed programs select the program **USB-Blocker** and click on **Uninstall**.
3. Follow the instructions of the program.

3.2 Operating the Program

The program operation is quite simple and includes three steps:

1. Create groups

For every device, every class, service etc. that should be monitored, a group with corresponding name has to be created on the computer or in the domain.

As soon as this group exists, the **bi-Cube[®] USB-Blocker** permits access only to members of this group.

2. Administer memberships

Decline or permit users to use the monitored devices by adding or removing them to/from a created group.

3. Configure the **bi-Cube[®] USB-Blocker**

The method of the USB-Blocker service can be changed by various configurations. Example:

- assigning of users for group inquiry,
- group prefix defining,
- the log activity settings,
- NDS support activation and configuration.

3.2.1 Creating Groups

Prior to creating groups to monitor devices, develop your strategy of hardware monitoring and controlling.

3.2.1.1 Preliminary considerations

The following considerations are important:

1. Each device can be assigned to various groups.
2. To block a device, at least **one** of these groups must be available.
! The existence of only one of these groups leads to the blocking of devices!
3. To enable the usage of a monitored device to a user, the user must be a member of at least **one** of these groups.
4. Groups can apply to only one device or they can be overlapping, thus applicable for several devices.
5. To every connected device, five properties are determined by the **bi-Cube[®] USB-Blocker**:
 - a) Device service
 - b) Device class
 - c) Device class description
 - d) Device name
 - e) Device ID
6. To secure the unique identification of devices, these properties can be combined.
7. Due to wild card characters it is possible that different USB sticks of the same chip set producer can be released in only one group. In order to phrase the wildcards "asterisk" and "question mark", character combinations can be defined.
8. Internal devices are disabled by the **bi-Cube[®] USB-Blocker**. It is to be noted that the device ID of apparently independent system devices can be identical. This can lead to an unintended device blocking. It is recommended to block not via the device ID but by device classes and/or device services.

Please, note that the blocking of internal hardware components can possibly lead to a system shut down. Therefore please first test your settings on a computer that is offline.

The following options are available to create two special groups.

1. HW_TRUSTED
 - Members of this group can use all devices without restrictions.
 - The existence of just these groups has no effect.
2. HW_NOTRUSTED
 - All devices without exception are blocked for members of this group. The usage of devices has to be permitted.
 - Members of this group who are also a member of the SystemHardwareLock group (created for the corresponding system) are not able to change the hardware on this PC.
 - The existence of just these groups has no effect.
 - Note:
! ALL devices, which means in this case really ALL!
This corresponds to not only USB, HDD, CD-ROM etc. but also mouse, keyboard, display, everything that is listed in the Windows Device Manager.

The success of your strategy depends on the well-deliberated combination of possibilities.

For example by creating a group, the USB mass storage is blocked globally and single USB mass storage can be permitted by special device groups.

3.2.1.2 Determine group names

Group names can be determined with the program **USB-Blocker Admin**.

Start the program USB-Blocker Admin:

To launch the program USB-Blocker Admin click on **Start**, then **All Programs** select **USB-Blocker** and then click on **USB-Blocker Admin**.



Picture 1 USB-Blocker Admin

In the left part of the program user interface, the device structure of the installed and connected devices of your computer is displayed. It corresponds to a Windows Device Manager.

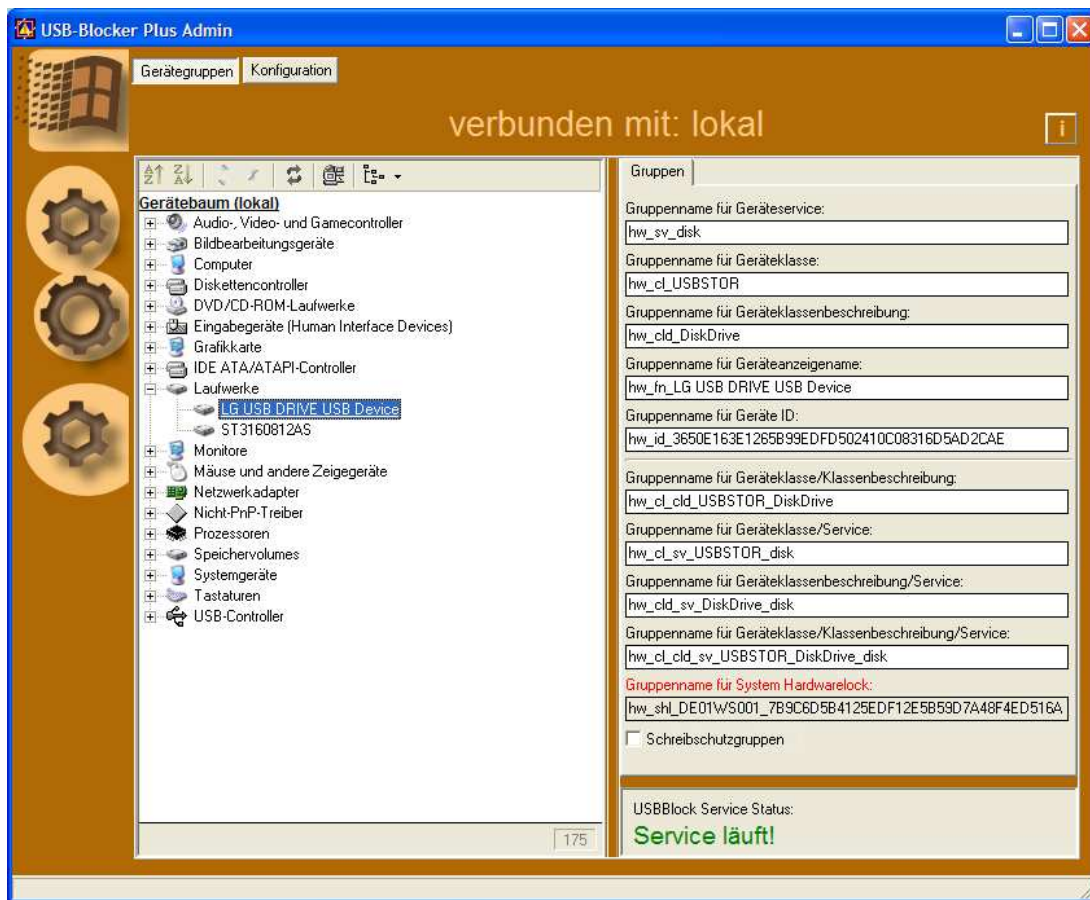
Using the symbol bar, you are able to:

- change the sorting and the structure view,
- refresh the view manually and
- establish a remote connection to a computer of your network.

The display of locally available devices is refreshed automatically with every hardware change.

→ Apply the devices you want to monitor to your computer or remotely connect to a computer to which the device is attached.

→ Go to every device in the structure for which you want to determine a device name.



Picture 2 Detailed view of devices

Possible group names are displayed in the detailed view, to the right.

The first five group names are generated directly from the device properties:

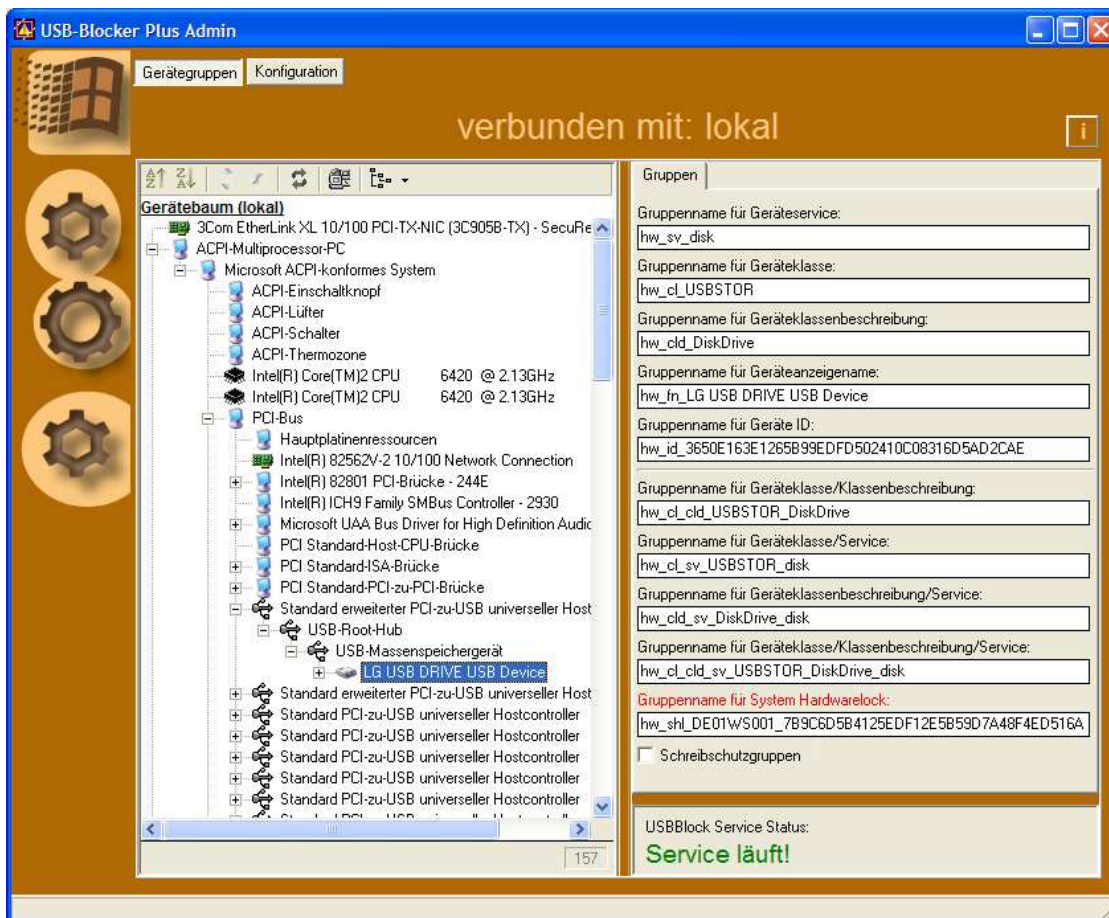
1. Device service
2. Device classification
3. Description of device classification
4. Name of device display name
5. Device ID

The four additional group names are combined from these properties.

Example: An USB flash drive is listed:

4. as an USB mass storage below USB Controller
1. as <display name> at the drives
2. as a standard volume at Drive volumes

To better illustrate these connections, switch to the view **Display devices by connection**.



Picture 3 Display of devices by connection

Every entry is a separate device and thus can be blocked. Devices depended on this device are also affected by the blocking unless they are released. Select the group name(s) according to your planned locking strategy.

3.2.1.3 Restrict writing rights

With the **bi-Cube[®] USB-Blocker** the writing access on data media can be restricted. If a device can be write-protected, it will be displayed by the check box "**Write protection groups**".

If this option is activated, the displayed group names will end with the suffix **01**. When the **bi-Cube[®] USB-Blocker** identifies a device with a write protection group then no data can be written to this corresponding device.

For members of a write protection group, the write-protection is disabled.

For members of a regular blocking group, only reading access is available.

If for the same device no regular blocking group exists, then all who are not a member in the write protection group, the read-only is authorized.

3.2.1.4 Naming conventions

The **USB-Blocker Admin** displays the group names with a prefix:

- | | |
|---|---------|
| 1. Device service | hw_sv_ |
| 2. Device classification | hw_cl_ |
| 3. Description of device classification | hw_cld_ |
| 4. Name of device display name | hw_fn_ |
| 5. Device ID | hw_id_ |

For the combination of group names, the prefixes are also combined accordingly.

These prefixes can be freely selected and this makes the group management easier. You can customize these prefixes in the USBBlock.ini according to your needs.

3.2.1.5 Manage memberships

The authorization to use hardware devices is controlled via the membership in local or domain groups. In order to grant access for a user, he has to become a member of this local or domain group.

To execute some of these tasks you have to be logged on as the **Administrator** or as a member of the group **Administrators**.

The example below describes the procedure by using the computer management of the Windows XP Professional.

In several operating systems there are a number of administration and command line programs; by using them you can perform this task. See also the help option of each appropriate operating system.

3.2.1.5.1 How to set up a local group

1. Open the **Computer Administration**.
2. Find **Groups** in the console structure.
 - o Computer administration
 - o System program
 - o Local users and groups
 - o Groups
3. Click on **Action** and then on **New Group**.
4. Enter a new name for the new group in the **Group Name** field.
5. Click on **Create** and then on **Close**.

Notes

- To open the Computer administration, click on **Start** and then click on **System control**. Click on **Performance and Maintenance**, click on **Management** and double-click on **Computer administration**.
- The name of a local group cannot be identical with any other group or user name on the used computer. The name can contain up to 256 small or capital letters and characters with exception of the following: " / \ [] : ; | = , + * ? < >
- The name domain group can contain all Unicode characters, except of the special LDAP characters according to RFC 2253: first or following space, as well as the special characters # , + " \ < > ;
- A group name cannot be built only of dots (.) or spaces.

3.2.1.5.2 How to delete a local group

1. Open **Computer administration**.
2. Find **Groups** in the console structures.
 - Computer administration
 - System program
 - Local users and groups
 - Groups
3. Click with the right mouse-button click on the group you want to delete and then click on **Delete**.
- 4.

3.2.1.5.3 How to add a member to a group

1. Open **Computer administration**.
2. Find **Groups** in the console structures.
 - Computer administration
 - System program
 - Local users and groups
 - Groups
3. Click with the right mouse button on the group to which you want to add a member, point to **All Tasks**, click on **Add member** and then click on **Add**.
4. Click on **Search in** to see a list of domains in which users and groups can be added to a group.
5. Click under **Path** on the domain with users and computers that you want to add and then click on **OK**.
6. Enter the name of the user or group you want to add into the **Name** field and then click on **OK**.

If you want to recheck the added user or group names, click on **Check names**.

3.2.1.5.4 How to delete a member from a group

1. Open **Computer administration**.
2. Find **Groups** in the console structures.
 - Computer administration
 - System program
 - Local users and groups
 - Groups
3. Click with the right mouse button on the **group** from which you want to delete a member.
4. From the field **Member** select the user you want to delete from the selected group. Click **Delete**.

3.2.1.6 Windows XP Home Edition

In Windows XP Home the required administration panels are not available. Instead you can use the net-commands for the group management.

- Check the available local groups:

```
net localgroup
```

- Create a USB-Blocker device group:

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

- Add a user/group to a USB-Blocker device group:

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

- Check the members of the USB-Blocker device group:

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

3.2.2 Configuring the **bi-Cube[®]** USB-Blocker

In the window **USB-Blocker Admin** you may switch between the view *Device groups* or *Configuration* of device groups.

When you are remotely connected to a computer you can view and change the device groups or also the configuration of the **bi-Cube[®]** USB-Blockers.

Important: For the configuration, the program has to be started with local administrative rights!



Picture 4 Switching between program views

3.2.2.1 **bi-Cube[®]** USB-Blocker Admin user

In this area, the local **Windows user** used by the **bi-Cube[®]** USB-Blocker can be changed. This service account is created during installation and equipped with a random password. The user owns administrative rights which are required to delete devices from the system when they have been blocked.

The user, used by the **bi-Cube[®]** USB-Blocker can be changed. However, he must own local administrative rights. Local and domain users can be used. To change the Admin user is optional.

Important: To change this data should only be required for special scenarios, since this could lead to that the **bi-Cube[®] USB-Blocker does not function properly anymore.**

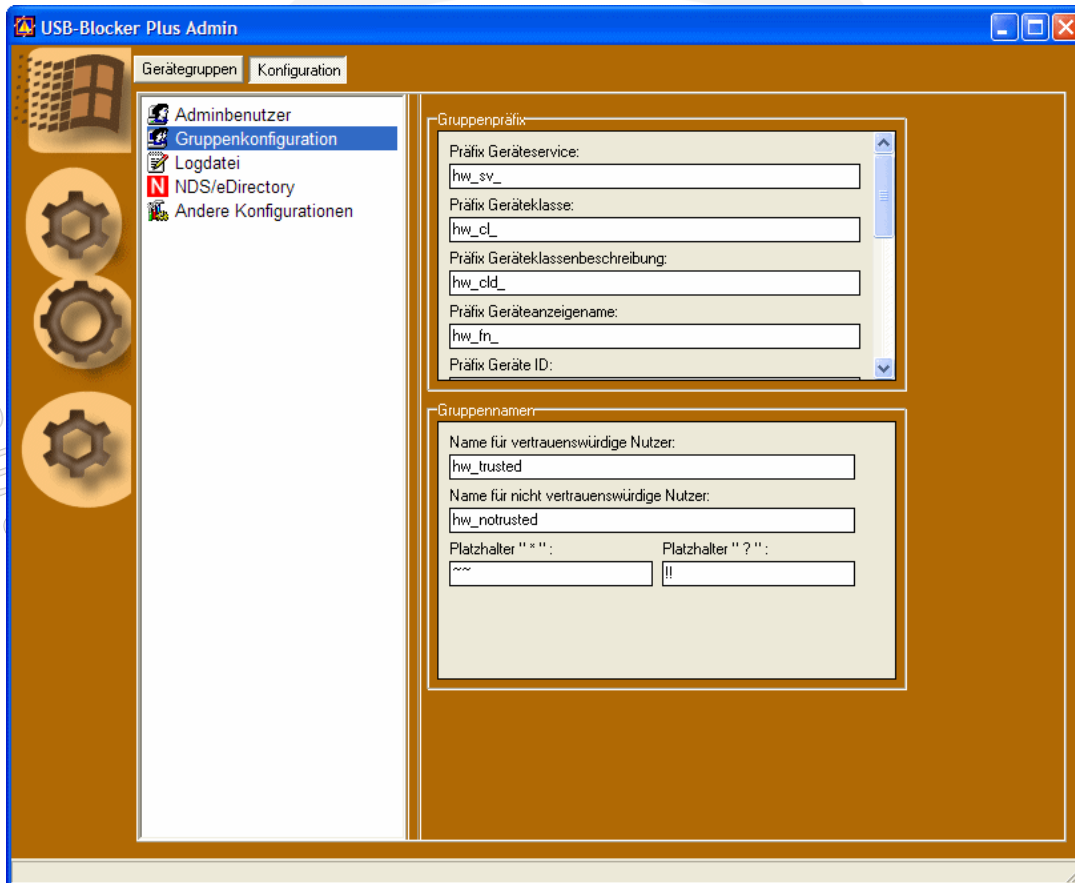
Important: To change this data should only be required for special scenarios, since this could lead to that the **bi-Cube[®] USB-Blocker** does not function properly anymore.



Picture 5 Settings for USB-Blocker Admin User

3.2.2.2 Settings for group configuration

Each group for the **bi-Cube[®] USB-Blocker** depends on an adjustable schema. A prefix is already predefined for all groups. In this case these group prefixes can also be adjusted to own nomenclatures for groups of USB-Blocker Admin. Changing of this setting is optional. We recommend you leave these settings unchanged.



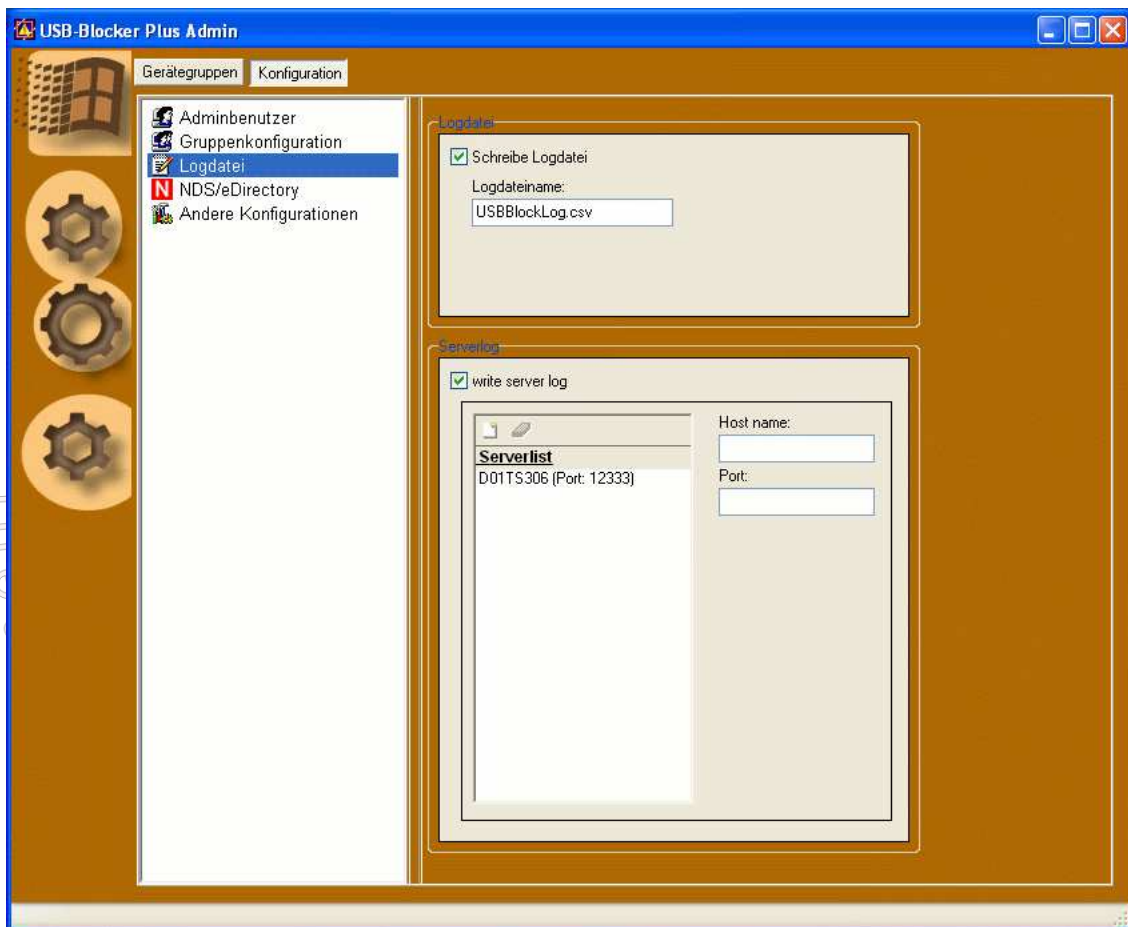
Picture 6 Settings for group configuration

3.2.2.3 Settings for the **bi-Cube[®] USB-Blocker** log activity

At this part of the Admin Tool the log activity of the **bi-Cube[®] USB-Blockers** can be configured.

When this option is activated then all activities of the **bi-Cube[®] USB-Blockers** are written to a log file. This includes the registered user, all determined blocking groups, the blocking group to which the user is a member and all other **bi-Cube[®] USB-Blocker** events like inserting a USB device. The data is saved as a .csv format to the selected file. Name and path of the log file can be customized.

In addition, the **bi-Cube[®] USB-Blocker** provides the option to centrally save the log data in a database. For this, the server name and the port of the ZAM server service must be indicated. This feature is only available with **bi-Cube[®] Extended**.



Picture 7 Settings for log activities

3.2.2.4 Settings for NDS support

Settings represented in this view are necessary for proper cooperation of the **bi-Cube[®] USB-Blocker** with the **NDS/eDirectory**. After installing the **bi-Cube[®] USB-Blockers** the option "use Novell" is deactivated as default.

After activating this option, the following configurations are possible:

a) Use Admin user for the NDS connection (ZEN)

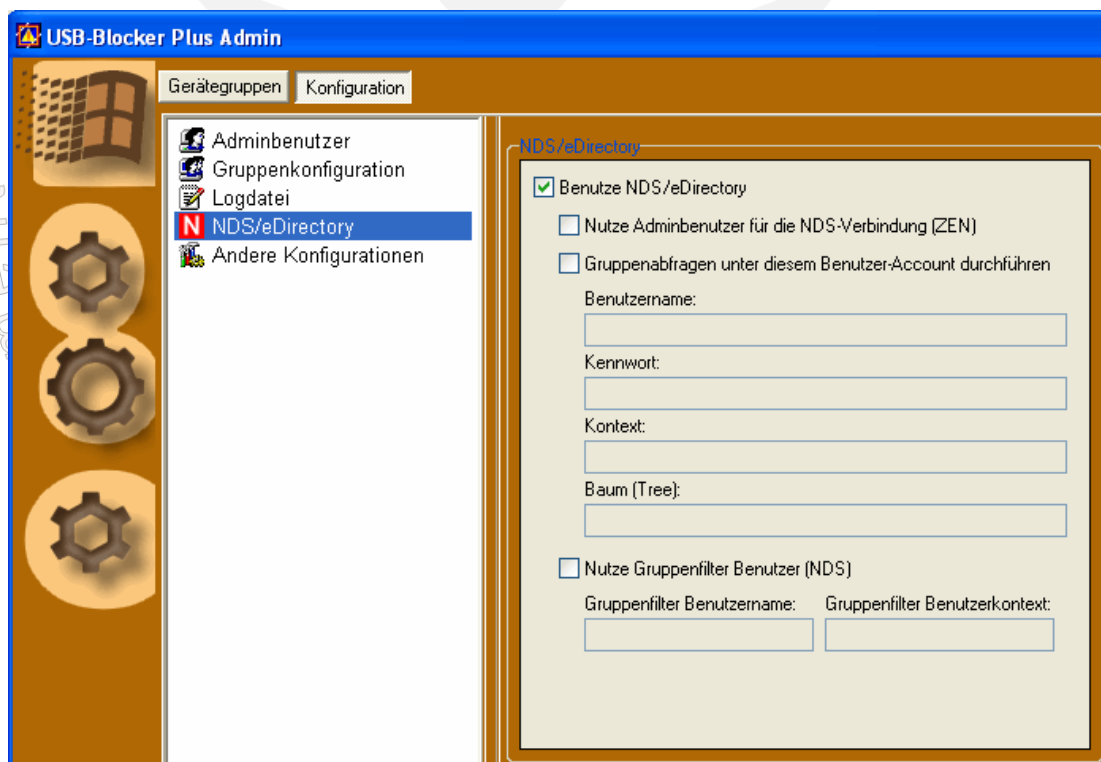
If the software distribution ZENworks is used, this option should be activated, because otherwise problems by interacting with the ZENworks client could occur. By activating the option, the admin user, defined by the USB-Blocker Admin is used to establish a connection.

b) Use this user account for group queries

This option allows you to specify a defined user account (optionally), by whose rights all required queries in the NDS are executed.

c) Use group filter user (NDS)

By activating the group filter User the search for groups in the NDS is shortened. The group members of the selected user account are used as blocking groups. However, if the group filter User is not member of a group, it cannot be used for blocking.
(The activation of: Use group filter user, is recommended).

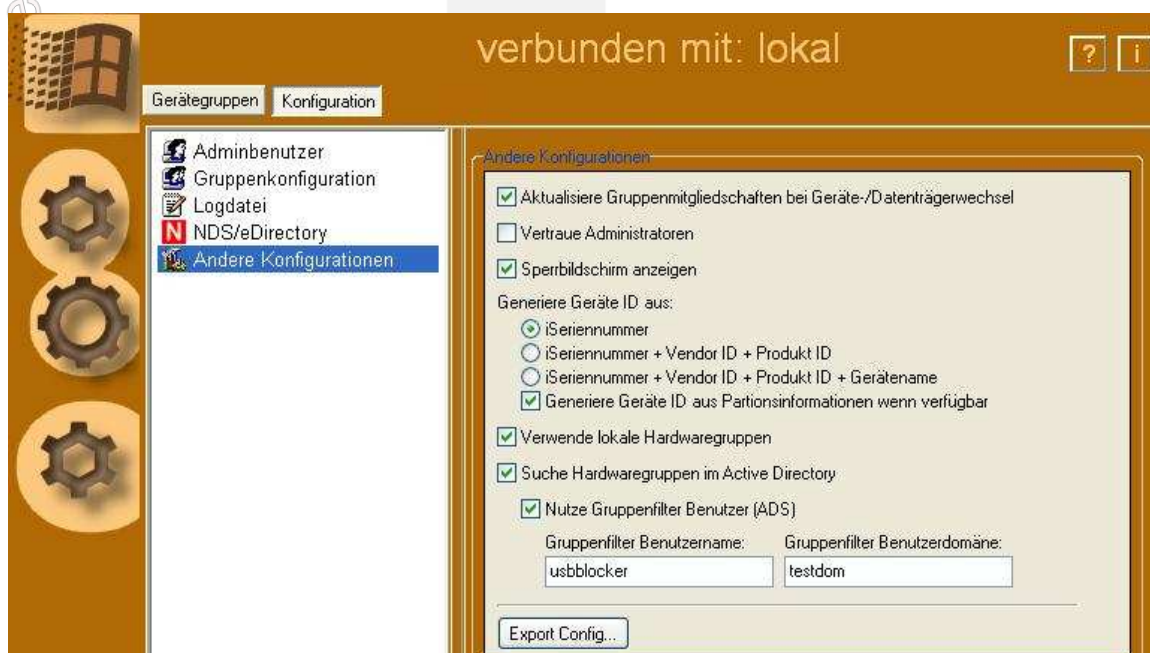


Picture 8 Settings for NDS/eDirectory Support

3.2.2.5 Settings for additional parameters

The options points in the field **Other Configuration** have the following meaning:

- a) **Refresh group memberships at device/data medium change** means the **bi-Cube[®] USB-Blocker** refreshes the group configuration for every enabling or removing of a device or a data media. The available groups in AD/NDS and local defined groups are loaded again. This is useful when the user memberships change frequently in the groups. The user does not need to log him self off and on when refreshing.
- b) The option **Trust administrators** deactivates the block function for users with administrative rights independent from the existing device group.
- c) **Display screen lock** activates the lock screen which appears during the device eject. This is a default setting.
- d) The configuration option **Generate device ID of** is used for the setting of the generation algorithm of the device ID group. In some cases it happens that Windows assigned the same ID to different external devices. In such case it is necessary to improve the identification process. The generation of the device ID group with the iSerial number is preset. If this setting is not sufficient for a clear identification, you can create a more defined group by adding additional device properties. At chapter 2 next to the iSerial number also the **Vendor ID** and **Product ID** is used for generating the device ID. At chapter 3 also the device name is included. At the mass storage media, mentioned in chapter 4, the partition-information to generate the device ID is added.
- e) Activate **Use local hardware groups**, if a locally applied device groups should be considered. It is recommended, to deactivate this option while using AD or Novell.
- f) Check mark the **Search hardware groups in Active Directory**, if you want to centrally manage the device groups in the AD.
- g) When you activate the option **Use group filter user (ADS)** then the search of groups in the Active Directory is shortened. The group members of the selected user account are used as blocking groups. If the **Group filter user name/domain** is not member of a group, it cannot be used for blocking. *(The activation of: Use group filter user (ADS), is recommended)*
- h) With the button **Export Config...** you may export current configurations to a reg-file which is used for the software distribution or for the manual transfer of configurations.



Picture 9 Settings for additional parameters

3.2.3 Group administration in NDS

After activating the option to connect the **bi-Cube[®] USB-Blocker** to the **NDS** and completion of the configurations as described in [3.2.2.4](#), the **bi-Cube[®] USB-Blocker** reads out the appropriate user groups in the NDS. If the option **Group filter user name/domain** should not be used, it is described in the following which versions of affiliations of users within the groups are possible.

3.2.3.1 Possible group constellations

The **bi-Cube[®] USB-Blocker** can analyze groups and users subordinate to the organization and in OU's during an activated NDS connection. This results in the following constellation in memberships:

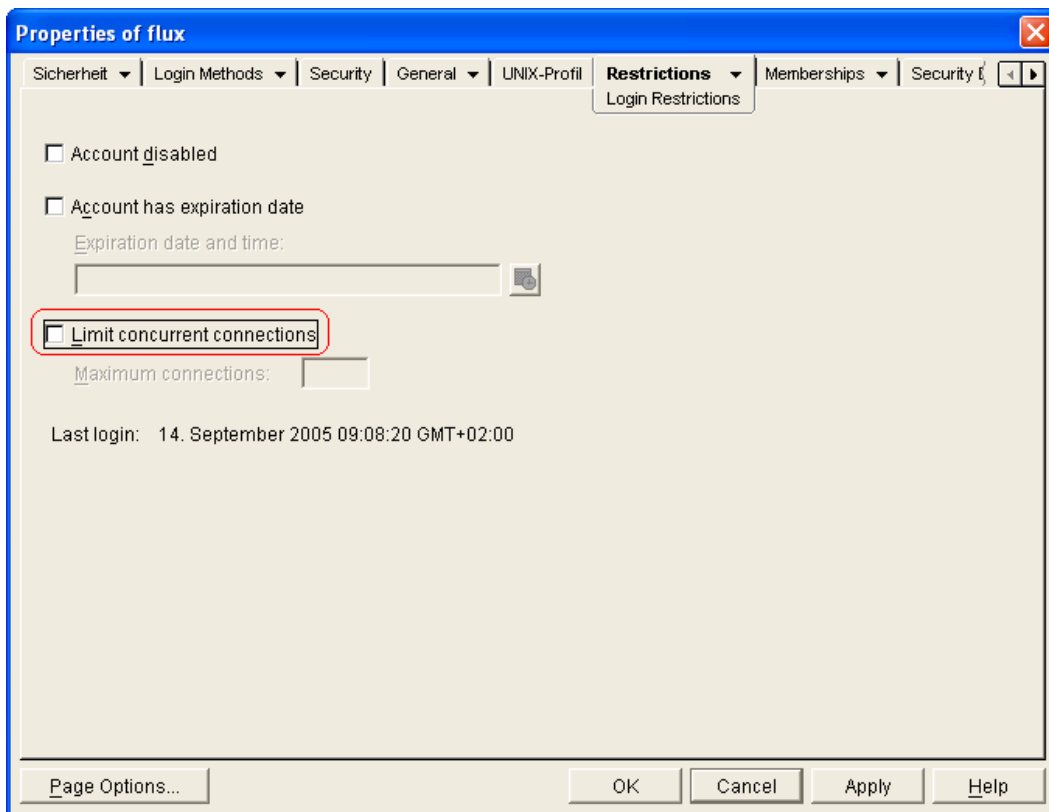
1. The user is created subordinate to the organization.
 - a) The user is a member of a group which was also created subordinate to the organization.
 - b) The user is a member of a group which is part of an OU.
2. The user has been created within an OU.
 - a) The user is a member of a group which was also created subordinate to the organization.
 - b) The user is a member of a group which is located in the same OU as the user.
 - c) The user is a member of a group which is located in another OU than the user.

3.2.3.2 Configuration hints for the NDS usage

It is recommended to install the USB-Blocker Admin on one computer from which an administration access (ConsoleOne, Web administration) to the NDS is possible. The groups for administration of the devices and users have to be set-up in the NDS manually.

Note:

For the in section [3.2.2.4](#) described administrative Novell user the following should be considered: So that the **bi-Cube[®] USB-Blocker** can execute competing (simultaneously) queries for groups in NDS with the specified user, there should be no logon restrictions for this user.



Picture 10 Settings for the administrative NDS user

3.3 Installation via software distribution

To facilitate the installation in a network, the **bi-Cube[®] USB-Blocker** can be distributed to client workstations via systems for software distribution.

Via a software distribution a Windows 2000/2003 domain distributable **MSI-file** and **MST-file** including licensed data are provided by the manufacturer. The installation of **InstallShield Script-Engine 8** is only necessary, if the installation on the clients with corresponding error message written to the application log file has failed.

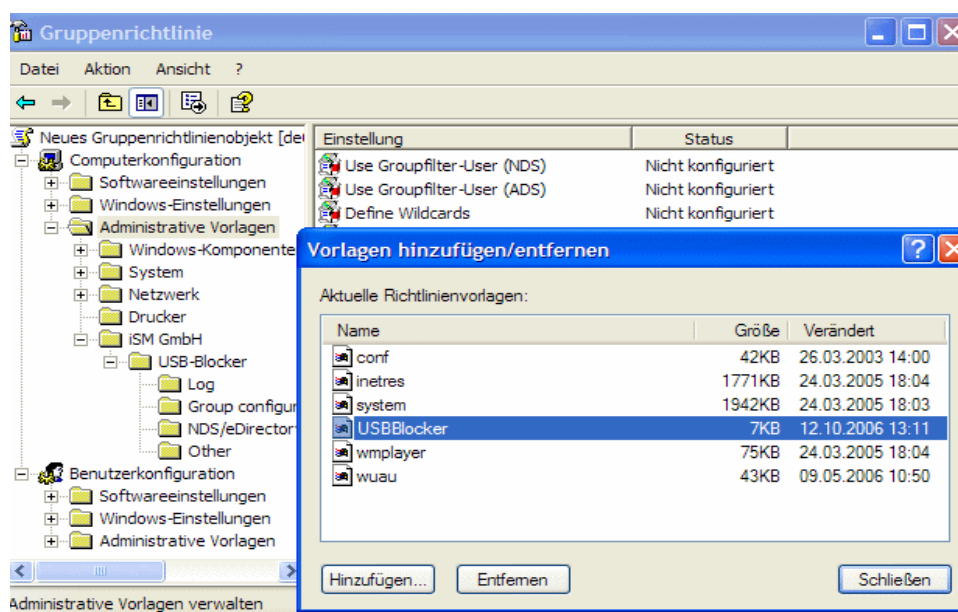
The exported (by the USB-Blocker Admin) configuration file **usbblock.reg** ([3.2.2.5](#)) is also transferred to the clients via software distribution. For this, the file must be stored in the same folder as the MSI-package to be distributed and these are at installation used automatically.

3.4 Administration of **bi-Cube[®]** USB-Blockers via Group Policies (GPO)

After installing the admin interface the **bi-Cube[®] USB-Blocker** installation directory contains an **ADM-file** which can be integrated into a **GPO**. This enables to comfortably change the configuration of the **bi-Cube[®] USB-Blockers** at the clients.

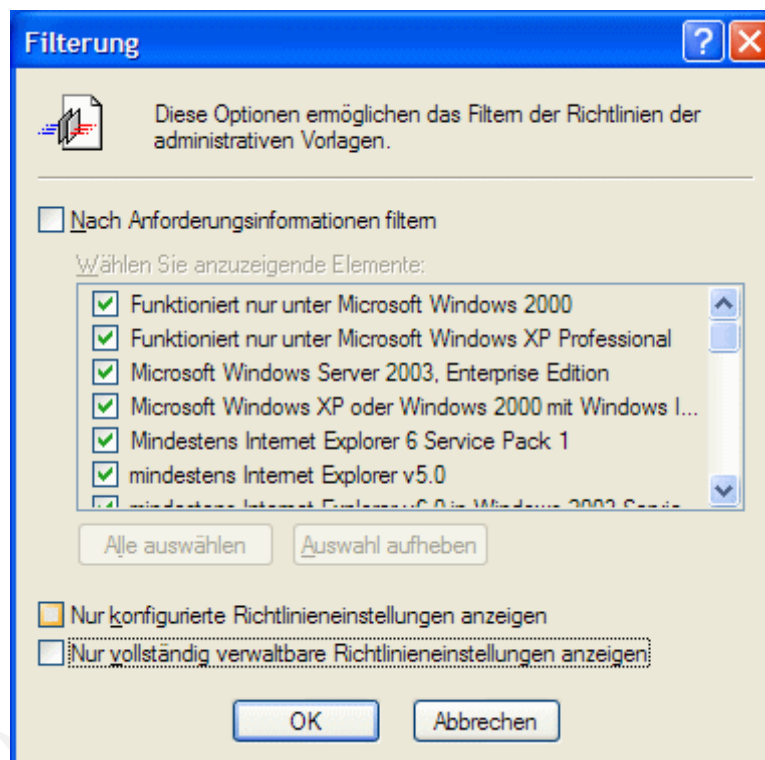
Copy the ADM-file to the directory: C:\Windows\inf of the domain controller. Open the **Group Policy** editor and create a new GPO.

Open the **GPO** and with the right mouse button click in the category **Computer configuration** on **Administrative templates**, select **Add/delete template** and add the USB-Blocker-ADM as template.



Picture 11 Group policy – Editor Group policy editor

Since the **bi-Cube[®] USB-Blockers** policy settings are not fully administrable policy settings, a accordant filter must be deactivated by removing the check mark from the corresponding option at **administrative templates** category.



Picture 12 Filtering policy settings

Management - Institut für System-Management
Copyright by ISM-Instiut für System-Management

3.5 **bi-Cube[®] USB-Blocker 30 Days Trial Version**

During the trial phase of 30 days, the **bi-Cube[®] USB-Blocker** can be used without any restrictions.

At each start of the **USB-Blocker** and/or the **USB-Blocker Admin** an info window is shown for 120 seconds. You may close this window at any time by clicking the **Close** button.



Picture 13 Info window

After the expiry of this testing phase, the service **USB-Blocker** cannot be launched anymore. While trying to start the service again, it will be closed automatically. You will be informed about this process in the system event protocol.

After this time period, all users can use the workstation again without restrictions. A membership check for the defined groups is not executed anymore.

4 Results - Example of configuration

Intention of this example configuration is the deactivating of all USB-mass storage media. USB devices, which are not a mass storage media, will continue. Additionally a special USB-stick should be released.

Please keep the default data for non mentioned settings of the exemplary configuration.

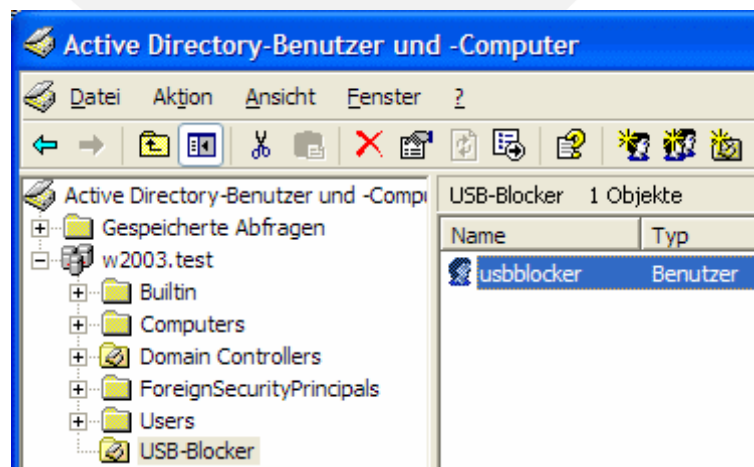
It is preconditioned that the **USB-Blocker Admin** is installed on the testing workstation and that a USB stick is plugged in and is operational. Furthermore write access to the **Active Directory** or **eDirectory** is required.

To implement the following steps the **USB-Blocker Admin** needs local admin rights.

4.1 Active Directory

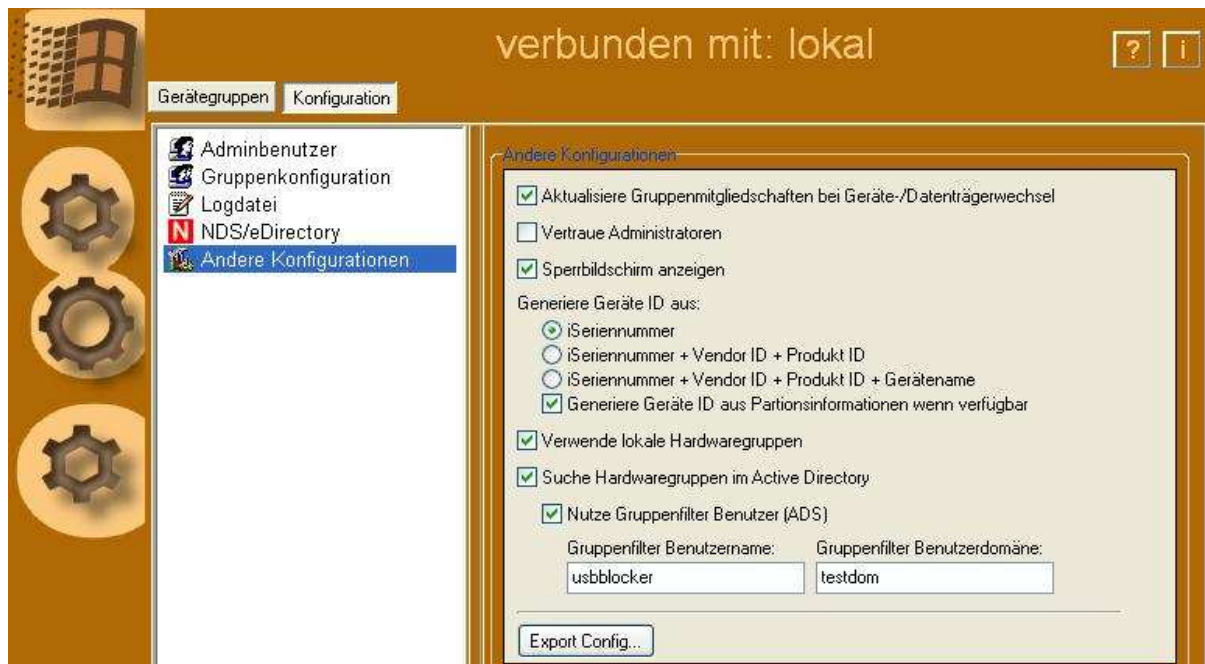
Please do the following:

1. Open the console **Active Directory-User and -Computer**.
2. Create a new Organizational unit (OU), e.g. with the name "USB-Blocker".
3. In this OU create a new user, e.g. usbblocker. Deactivate the account option **User must change password at next logon**, then activate the option **Password never expires**.



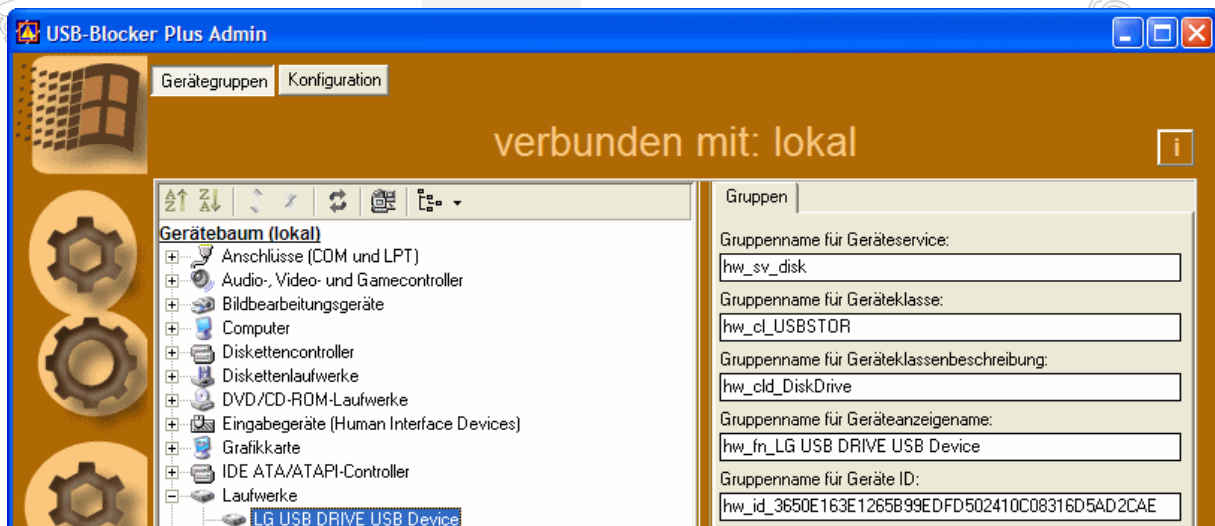
Picture 14 Creating a AD-user

4. Keep the console opened and start the **USB-Blocker Admin** via the Start menu.
5. Switch to the configuration view by clicking the button **Configuration**.
6. Click on **Other Configurations**.
7. Activate the option **Use Group filter User (ADS)**.
8. Enter the previous created user **usbblocker** and the domain.



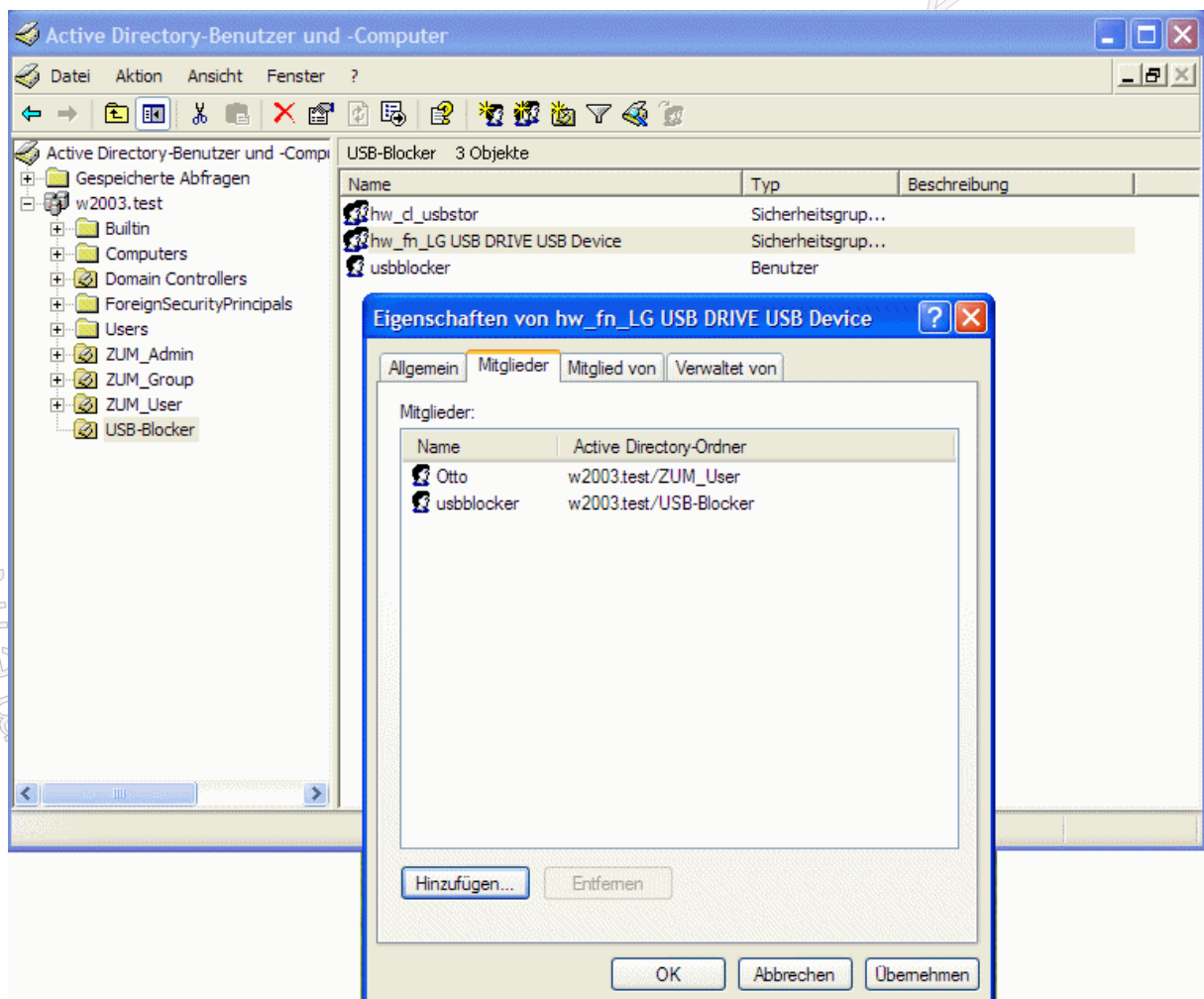
Picture 15 Activating *Use Group filter User (ADS)* and entering user name and domain

9. By the button **Device groups** switch to the device tree structure view of the **USB-Blocker Admin**.
10. Click on the knot **Drives (Windows XP)** or **Data medium (Windows 2000)**.
11. Click on the USB-Stick you want to release.
12. Into the field of the right sub-window **Group name of device classification** copy: **hw_cl_usbstor**
 This group name describes all devices of the classification USB-mass storage.



Picture 16 Entering the AD *Group name of device classification*

13. Change to the console **Active Directory-User and -Computer** and create a group **hw_cl_usbstor** in the OU of the **USB-Blocker**. Global and universal groups of the type security are supported.
14. Switch to **USB-Blocker Admin** and copy to the right the **Group name of device display name: hw_fn_LG USB DRIVE USB Device**
The group name only represents the currently inserted device or other similar devices.
15. Apply this group also to the AD.
16. Assign the previously created user **usbblocker** as a member to both groups.
17. Assign the user e.g. Otto, who should receive authorization to use the device, as member to only the group **Group name of device display name**.



Picture 17 Assigning AD – member to the group *Group name of device display name*

18. Restart the service **USB-Blocker** to read the new authorization data.

Result: After restarting the service, the USB-stick will be ejected, as long as the logged on user (Otto) is not a member of the group **Group name of device display name**. After the logon with the user Otto, who is a member of the group **Group name of device display name**, the USB-stick can be used again. The device has to be plugged in again.

Reason:

In the described case a restrictive strategy is used. Generally all USB-Mass-storage media are blocked because of the group **hw_cl_usbstor**.

If a user is a member of the group, he is authorized to use the accordant device. The example shows that "Otto" became a member of the group **Group name of device display name**. Therefore the he is allowed to use the device.

Generally the following applies:

1. The **Group filter User (ADS)** must be a member of all groups relevant for the **bi-Cube[®] USB-Blocker**. This account should not be used for any other purposes.
2. The membership in a group permits the usage of the accordant device(s).

Note:

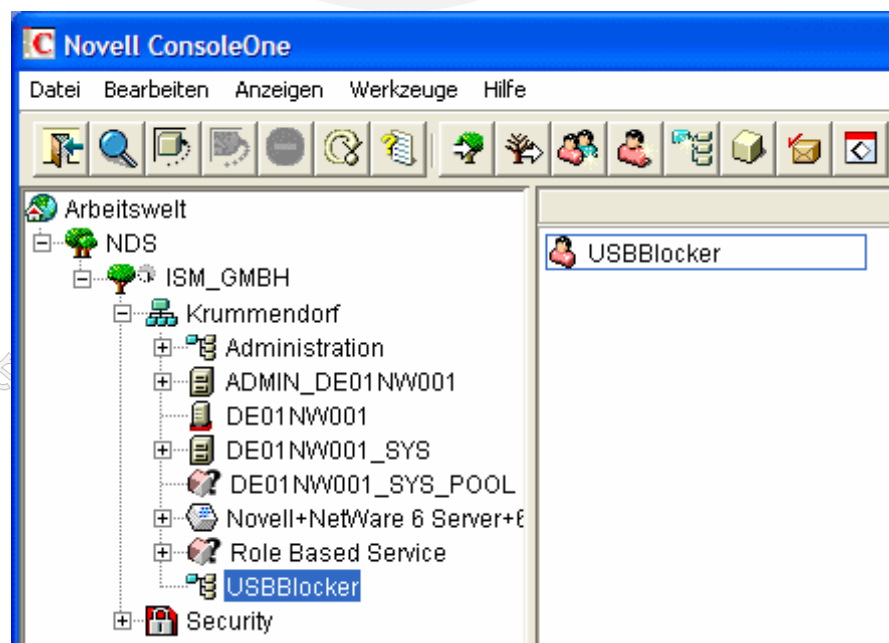
Group memberships in the AD take effect after a new logon.

Attention: If you wish to test the **bi-Cube[®] USB-Blocker** with its current settings on another computer, you must also transfer the configuration settings. Export the configuration as described in section [3.2.2.5h](#) and execute the reg-file on the client computer.

4.2 NDS/eDirectory

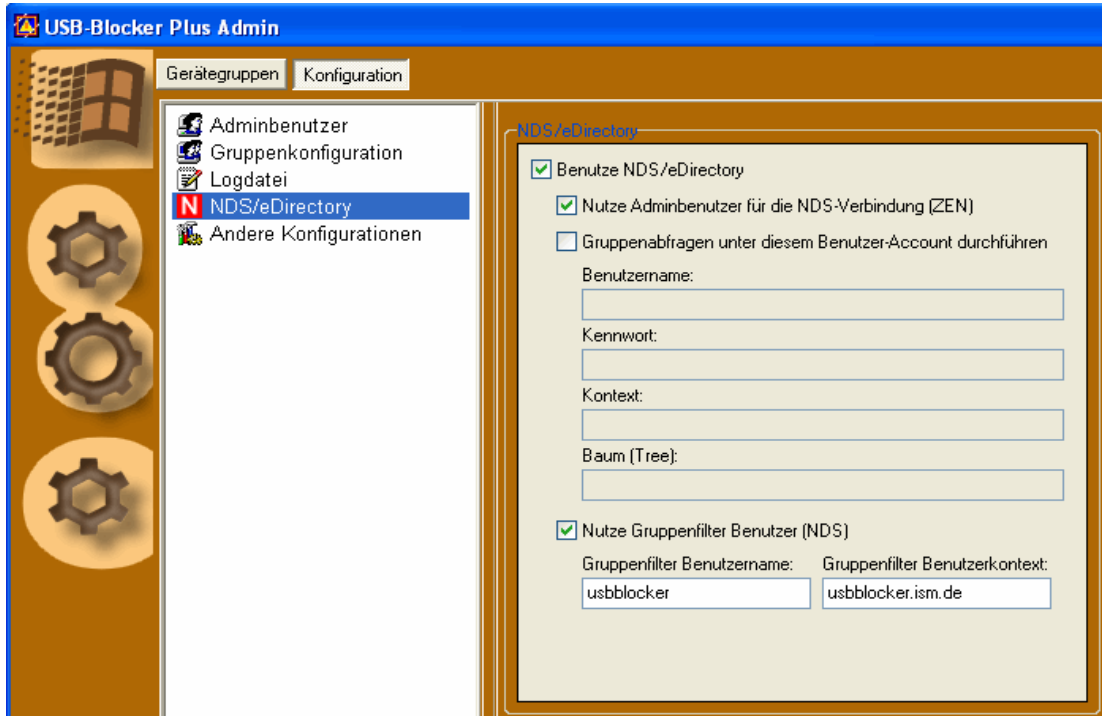
Do the following:

1. Open the Novell **ConsoleOne** and find your tree structure.
2. Create a new OU with the name, e.g. "USB-Blocker".
3. In this OU create a new user, e.g. **usbblocker**.



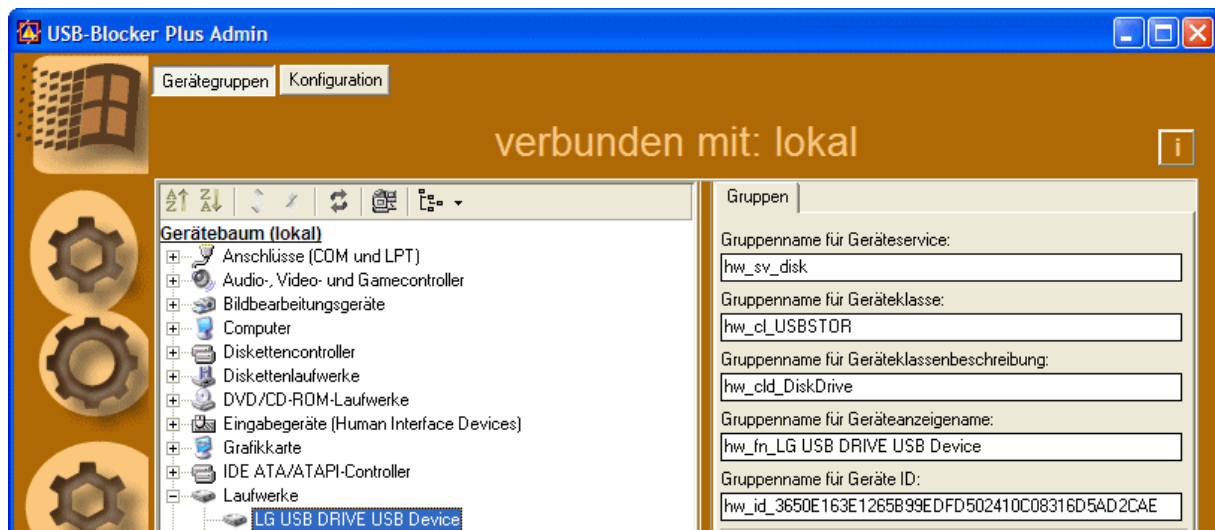
Picture 18 Creating new NDS – user to an OU

4. Keep **ConsoleOne** open and start the **USB-Blocker Admin** via the Start menu.
5. Switch to the configuration view by clicking the button **Configuration**.
6. Click on **NDS/eDirectory** and activate the option **Use NDS/eDirectory**.



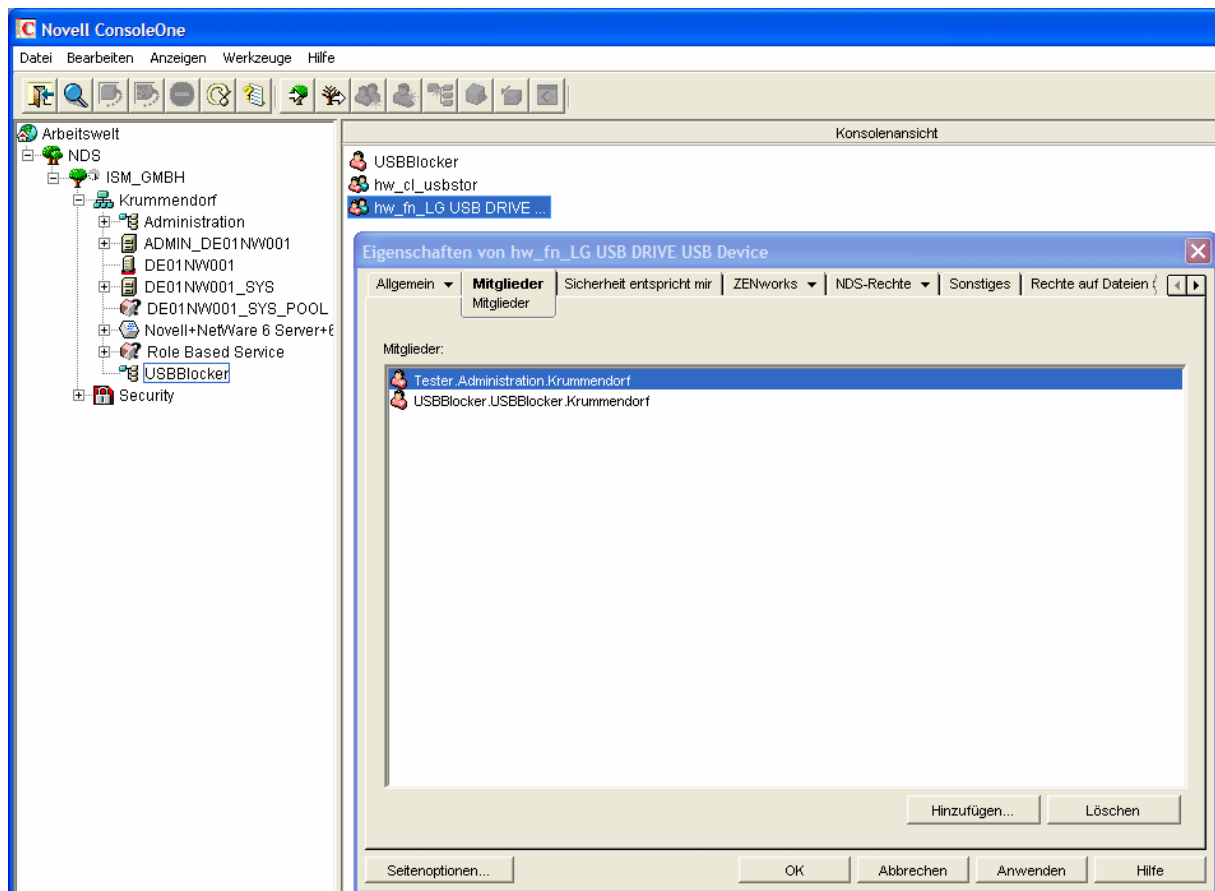
Picture 19 Configuration NDS/eDirectory

7. Activate the option **Use Group filter User (NDS)**.
8. In the given fields enter the previous created user **usbblocker** and his context (without tree structure!).
9. By the button **Device groups** switch to the device tree structure view of the **USB-Blocker Admin**.
10. Click on the knot **Drives (Windows XP)** or **Data medium (Windows 2000)**.
11. Click on the USB-Stick.
12. Into the field of the right sub-window **Group name of device classification** copy: **hw_cl_usbstor**
This group name describes all devices of the classification USB-mass storage.



Picture 20 Defining NDS – group name for device classification

13. Switch to **ConsoleOne** and create a new group **hw_cl_usbstor** in the OU of the USB-Blockers.
14. Change to **USB-Blocker Admin** and copy to the right the **Group name of device display name**, e.g. hw_fn_LG USB DRIVE USB Device
The group name only represents the currently inserted device or other similar devices.
15. Apply this group also to the **NDS/eDirectory**.
16. Assign the previously created user **usbblocker** as a member to both groups.
17. Assign the user e.g. Otto, who should receive authorization to use the device, as member to only the group **Group name of device display name**.



Picture 21 Defining NDS – member to the group *Group name of device display name*

18. Restart the service **USB-Blocker** to read the new authorization data.

Result: After restarting the service, the USB-stick will be ejected, as long as the logged on Novell-user is not a member of the group **Group name of device display name**.

After the logon with the user Otto, who is a member of the group **Group name of device display name**, the USB-stick can be used again. The device has to be plugged in again.

Reason:

In the described case a restrictive strategy is used. Generally all USB-Mass-storage media are blocked because of the group **hw_cl_usbstor**.

If a user is a member of the group, he is authorized to use the accordant device. The example shows that the "Tester" became a member of the group **Group name of device display name**. Therefore the he is allowed to use the device.

Generally the following applies:

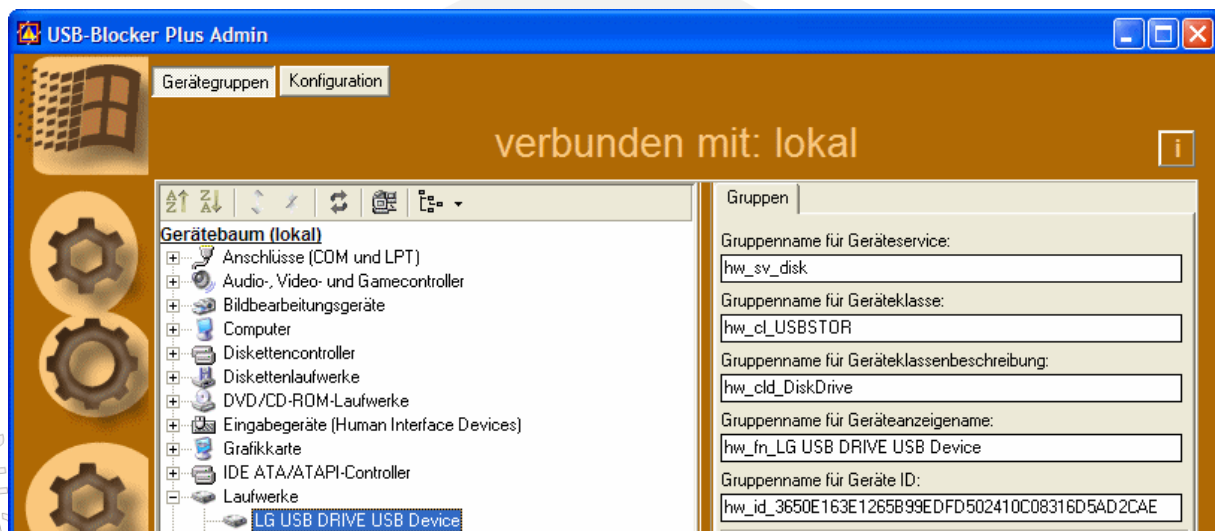
1. The **Group filter User (NDS)** must be a member of all groups relevant for the **bi-Cube® USB-Blocker**. This account should not be used for any other purposes.
2. The membership in a group permits the usage of the accordant device(s).

Attention: If you wish to test the **bi-Cube® USB-Blocker** with its current settings on another computer, you must also transfer the configuration settings. Export the configuration as described in section [3.2.2.5h](#) and execute the reg-file on the client computer.

4.3 Locally

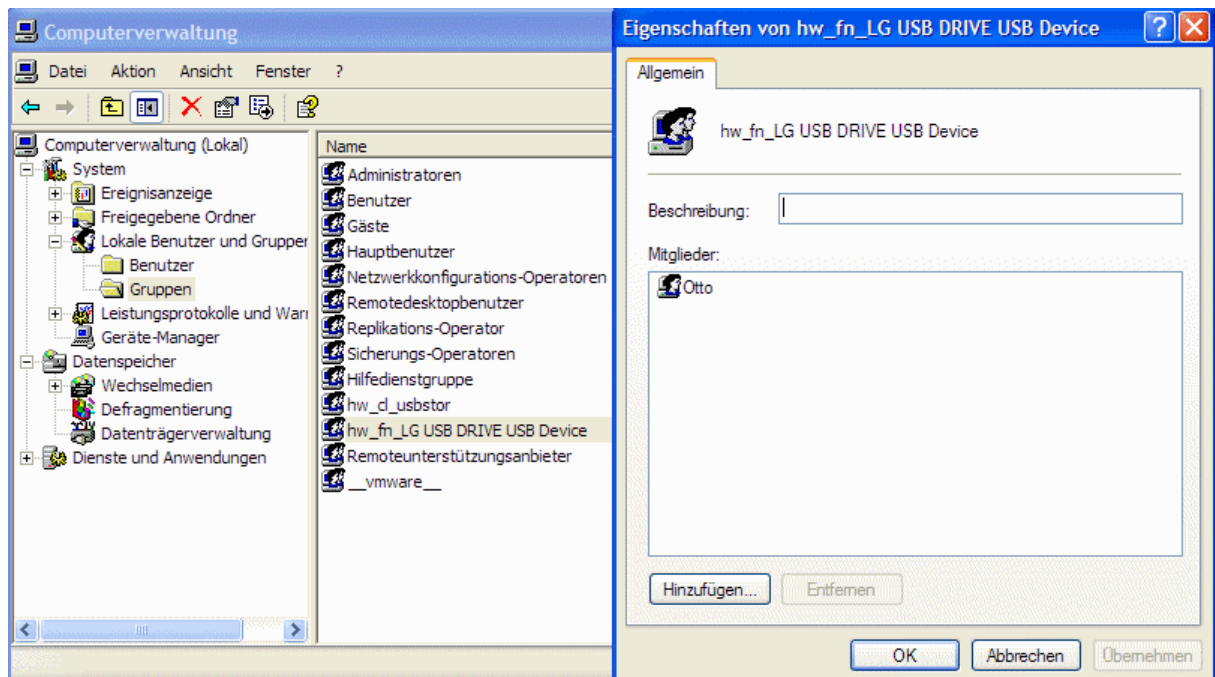
Do the following:

1. Open the **USB-Blocker Admin** via the Start menu.
2. Activate the option **Use local hardware groups** at **Configuration** → **Other configurations**
3. In the device tree structure click on the knot **Drives (Windows XP)** or **Data medium (Windows 2000)**.
4. Click on the USB-Stick.
5. Into the field of the right sub-window **Group name of device classification** copy:
hw_cl_usbstor
This group name describes all devices of the classification USB-mass storage.



Picture 22 Defining Local – group name for device classification

6. Open the local computer management and create the group **hw_cl_usbstor**.
7. Change to **USB-Blocker Admin** and copy to the right the **Group name of device display name**, e.g. hw_fn_LG USB DRIVE USB Device.
The group name only represents the currently inserted device or other similar devices.
8. Also create this group locally with the computer management console..
9. Assign the user e.g. Otto, who should receive authorization to use the device, as member to only the group **Group name of device display name**.



Picture 23 Defining Local – member to the group *Group name of device display name*

10. Restart the service **USB-Blocker** to read the new authorization data.

Result: After restarting the service, the USB-stick will be ejected, as long as the logged on Novell-user is not a member of the group **Group name of device display name**.

After the logon with the user Otto, who is a member of the group **Group name of device display name**, the USB-stick can be used again. The device has to be plugged in again.

Reason:

In the described case a restrictive strategy is used. Generally all USB-Mass-storage media are blocked because of the group **hw_cl_usbstor**.

If a user is a member of the group, he is authorized to use the accordant device. The example shows that the "Tester" became a member of the group **Group name of device display name**. Therefore the he is allowed to use the device.

Generally the following applies:

The membership in a group permits the usage of the accordant device(s).

4.4 Deactivate all USB devices

There are two options to disable USB devices:

4.4.1 Disable all USB device classifications

The following groups should be available:

hw_cl_USBSTOR	- blocks all USB mass storage media, cameras
hw_sv_USBPRINT	- blocks all USB printers
hw_cl_HID	- blocks all USB-human-interface-devices (mouse, keyboards)
hw_cld_Image	- blocks scanners, sensors, cameras
hw_sv_vmusb	- blocks the delivery of USB devices to virtual VMware guests
hw_cld_cl_USB_Net	- blocks USB network adapter
hw_cld_cl_USB_Bt	- blocks USB-bluetooth-devices

Now the groups related to the devices can be created to authorize the usage of certain devices.

This procedure is recommended.

4.4.2 Disable the USB hub

The following group should be available:

hw_cl_USB	- Blocks the USB HUB
------------------	----------------------

A user, who is authorized to use a USB device, has to be a member of this group, because the workstation cannot recognize the change in the device configuration, if the HUB is deactivated.

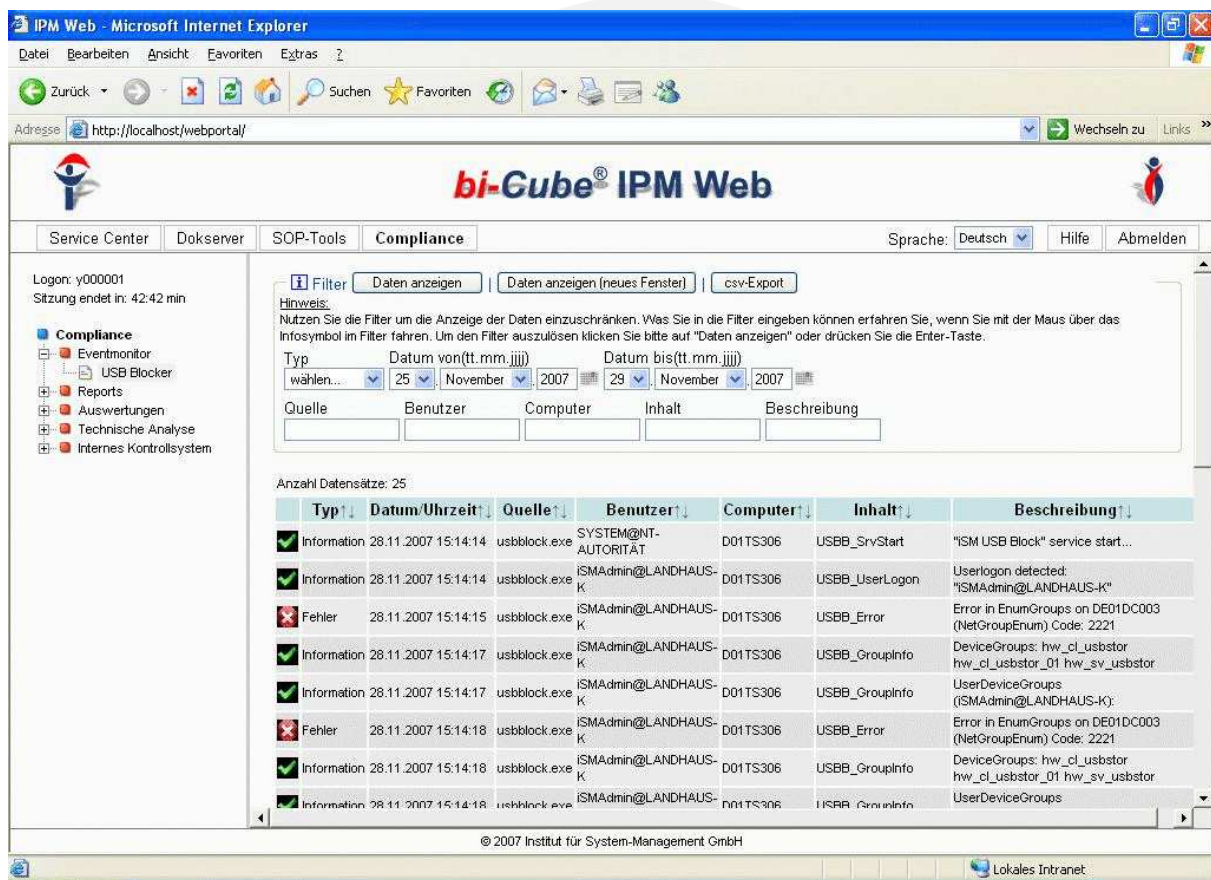
This procedure is recommended, if USB devices are never in use.

5 Extension of the **bi-Cube[®]** USB-Blocker functions with **bi-Cube[®]** IPM

The functions of the **bi-Cube[®]** USB-Blocker can be extended by using **bi-Cube[®]** IPM.

bi-Cube[®] IPM provides an automated and centralized control and management of the **bi-Cube[®]** USB-Blocker. Like the automated creation of device groups in the AD, a role model with many modeling possibilities and the monitoring of the Web interface are only some facilitations offered by the **bi-Cube[®]** IPM system administrator.

Thanks to the **bi-Cube[®]** modular system a customized solution can be offered to you.



The screenshot shows the 'bi-Cube[®] IPM Web' interface in a Microsoft Internet Explorer browser. The page title is 'IPM Web - Microsoft Internet Explorer' and the address bar shows 'http://localhost/webportal/'. The interface includes a navigation menu with 'Service Center', 'Dokserver', 'SOP-Tools', and 'Compliance'. The 'Compliance' section is active, showing a sidebar with 'Eventmonitor', 'USB Blocker', 'Reports', 'Auswertungen', 'Technische Analyse', and 'Internes Kontrollsystem'. The main content area displays a table of events with columns for 'Typ', 'Datum/Uhrzeit', 'Quelle', 'Benutzer', 'Computer', 'Inhalt', and 'Beschreibung'. The table contains 25 data rows, with the first few rows showing information and error messages related to USB-Blocker operations.

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	ISMAadmin@LANDHAUS-K	D01TS306	USBB_UserLogon	Userlogon detected: "ISMAadmin@LANDHAUS-K"
Fehler	28.11.2007 15:14:15	usbblock.exe	ISMAadmin@LANDHAUS-K	D01TS306	USBB_Error	Error in EnumGroups on DE01DC003 (NetGroupEnum) Code: 2221
Information	28.11.2007 15:14:17	usbblock.exe	ISMAadmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	DeviceGroups: hw_cl_usbstor hw_sv_usbstor
Information	28.11.2007 15:14:17	usbblock.exe	ISMAadmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	UserDeviceGroups (ISMAadmin@LANDHAUS-K):
Fehler	28.11.2007 15:14:18	usbblock.exe	ISMAadmin@LANDHAUS-K	D01TS306	USBB_Error	Error in EnumGroups on DE01DC003 (NetGroupEnum) Code: 2221
Information	28.11.2007 15:14:18	usbblock.exe	ISMAadmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	DeviceGroups: hw_cl_usbstor hw_sv_usbstor
Information	28.11.2007 15:14:18	usbblock.exe	ISMAadmin@LANDHAUS-K	D01TS306	USBB_GroupInfo	UserDeviceGroups

Picture 24 Central monitoring of the USB-Blocker

6 Notes

- In any case, test if the intended effect is reached and no other unintended incompatibilities (overlapping groups or compound devices) occur.
- It cannot be guaranteed that using of ascertained groups leads always to the same result.

7 FAQ

1. **Which group domain and type of group should be used for groups in the AD?**
 - a. *Global and universal groups of type Security are supported. This corresponds with the Microsoft recommendations concerning the group design in the AD.*
2. **Which account options must be activated for the group filter User?**
 - a. *Please ensure that the user does not have to change his password at initial logon and that the password never expires.*
3. **How does the .mst file be used for distribution so that the **bi-Cube[®] USB-Blocker** can be installed to the client with its licensed data?**
 - a. *In order to perform an uncontrolled installation and to use the .mst-file with the licensed data for the msi package, the following command must be executed:
„USB-Blocker Plus.msi TRANSFORMS=.mst-Datei /qb“*
4. **The lock screen disappears after a certain time period?**
 - a. *This is an intended procedure. The **bi-Cube[®] USB-Blocker** locks the workstation only as long as it is necessary to remove all blocked devices from the system. The input fields in the lock screen at bottom right are usually not required. By entering the administrator's account into the text box the screen can be released, in case a device cannot be removed.*
5. **How about the security in the safe mode?**
 - a. *The safe mode is not satisfying (although the name suggests otherwise) with the security by the **bi-Cube[®] USB-Blockers**.
In this mode only some few system drivers and services are loaded. The **bi-Cube[®] USB-Blocker** is not one of them. Consequently it is hypothetically possible to import or export files.
This problem concerns also viruses scan and firewalls etc. in a similar way. The only effective approach is to deactivate the network function of the safe mode, to avoid a logon via domain account (under the assumption that no local account is known to the user).
Z This can be achieved by renaming the key from:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
to e.g.:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Networkfals
e.*
6. **I have assigned a domain user as a member of a blocking group. Why can the released device still not be used?**
 - a. *Changes to group memberships are active in the Windows domain after a new logon.*

Directory – Pictures

Picture 1 USB-Blocker Admin	10
Picture 2 Detailed view of devices	11
Picture 3 Display of devices by connection.....	12
Picture 4 Switching between program views	15
Picture 5 Settings for USB-Blocker Admin User	16
Picture 6 Settings for group configuration.....	16
Picture 7 Settings for log activities	17
Picture 8 Settings for NDS/eDirectory Support.....	18
Picture 9 Settings for additional parameters.....	19
Picture 10 Settings for the administrative NDS user.....	21
Picture 11 Group policy – Editor Group policy editor.....	22
Picture 12 Filtering policy settings	23
Picture 13 Info window.....	24
Picture 14 Creating a AD-user	25
Picture 15 Activating <i>Use Group filter User (ADS)</i> and entering user name and domain	26
Picture 16 Entering the AD <i>Group name of device classification</i>	26
Picture 17 Assigning AD – member to the group <i>Group name of device display name</i>	27
Picture 18 Creating new NDS – user to an OU.....	28
Picture 19 Configuration NDS/eDirectory	29
Picture 20 Defining NDS – group name for device classification.....	30
Picture 21 Defining NDS – member to the group <i>Group name of device display name</i>	31
Picture 22 Defining Local – group name for device classification.....	32
Picture 23 Defining Local – member to the group <i>Group name of device display name</i>	33
Picture 24 Central monitoring of the USB-Blocker.....	35