

---

# User's Guide

**USB Blocker PLUS**

---

# Table of Content

<b>1</b>	<b>BRIEF DESCRIPTION .....</b>	<b>4</b>
1.1	How the USB-Blocker works .....	4
1.2	How secure is the USB-Blocker PLUS? .....	5
<b>2</b>	<b>PROGRAM INSTALLATION.....</b>	<b>5</b>
2.1	System requirements.....	5
2.2	Installing the USB-Blocker PLUS .....	6
2.3	Uninstalling the USB-Blocker .....	7
<b>3</b>	<b>PROGRAM HANDLING .....</b>	<b>7</b>
3.1	Creating groups.....	7
3.1.1	Deliberations.....	7
3.1.2	Group names ascertaining .....	8
3.1.3	NEW: Restrict writing rights.....	11
3.1.4	Naming conventions .....	12
3.1.5	Administering memberships .....	12
3.1.6	Windows XP Home Edition.....	14
3.2	Configuring the USB-Blocker.....	15
3.2.1	Settings for USB-Blocker Admin User .....	15
3.2.2	Settings for group configuration.....	16
3.2.3	Settings for log activity of the USB-Blocker PLUS .....	16
3.2.4	Settings for NDS Support .....	17
3.2.5	Settings for additional parameters.....	18
3.3	Group administration in NDS.....	20
3.3.1	Possible group constellations.....	20
3.3.2	Configuration hints for the NDS usage.....	20
<b>4</b>	<b>INSTALLATION VIA SOFTWARE DISTRIBUTION.....</b>	<b>21</b>
<b>5</b>	<b>ADMINISTRATION OF USB-BLOCKER VIA GROUP POLICIES (GPO) .....</b>	<b>21</b>
<b>6</b>	<b>USB-BLOCKER PLUS 30 DAYS TRIAL VERSION.....</b>	<b>23</b>
<b>7</b>	<b>EXAMPLE OF CONFIGURATION .....</b>	<b>24</b>
7.1	Active Directory .....	24
7.2	NDS/ eDirectory .....	27
7.3	Local .....	30
7.4	Deactivate all USB devices.....	31
7.4.1	Deactivate all USB device classes .....	31
7.4.2	Deactivate the USB hub .....	31
<b>8</b>	<b>IMPORTANT.....</b>	<b>31</b>
<b>9</b>	<b>FAQ .....</b>	<b>32</b>
<b>10</b>	<b>FUNCTIONAL WAY OF THE USB-BLOCKER PLUS .....</b>	<b>33</b>

© **Institut für System-Management GmbH**

Information to iSM products is liable to change service, but can vary in some irrelevant points of the functionality of current versions because of further development of the products. Persons and companies named in this document are fictitious for example purposes if not stated otherwise.

Copying or transferring of this document for any purposes (as well in extracts) is possible only after a written approval of iSM.

---

**Institut für System-Management GmbH**

Landhaus Krummendorf \* Oldendorfer Str. 12 \* D-18147 Rostock \* Germany

Telephone: +49 (0)381 37573-0 \* Fax: +49 (0)381 37573-29

Email: [info@secu-sys.de](mailto:info@secu-sys.de)

Internet: [www.secu-sys.com](http://www.secu-sys.com), [www.usb-blocker.com](http://www.usb-blocker.com)

# 1 Brief description

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

There have been various measures implemented in the past, 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. It cannot be made a difference between various USB devices, e.g. printers, hubs or USB flash drives.

The USB-Blocker in the Version 1.0 gave the possibility to administrate the using of USB mass storages depending on defined user rights.

With the now available **USB-Blocker PLUS**, new possibilities are open to administrate the using of almost any chosen hardware in your company. The popular USB devices are the main point of interest.

## 1.1 How the USB-Blocker works

The function of the USB-Blocker PLUS is very simple.

Every device in your computer disposes of various properties. A part of these properties can be shown when using the Windows Device Manager.

1. In order to open the Device Manager click on **Start**, then click on **System control**. Double click on **System**. On the **Hardware** tab, click on **Device Manager**.
2. Choose a hardware device in the shown structure, e.g. a DVD/CD-ROM drive of your computer
3. Click to show the device properties in the **Action** menu and then on **Properties**
4. On the **Details tab** a selection of the properties can be shown.

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

Separate devices also as a group of devices can be monitored by the USB-Blocker PLUS for their class or service affiliations etc.

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

Therewith the USB-Blocker PLUS controls access of a user on internal devices e.g. CD-ROM or disk drive.

The USB-Blocker PLUS supports the directory services Active Directory (ADS) and Novell eDirectory (NDS). Necessary connections are only built on, if it is required.

The program has to be installed on every workstation and set up as Windows service, which should be controlled. It starts automatically via Windows operating system.

**Note:**

The service USB-Blocker grants the controlling of the devices. Please take care that the user has no possibility to stop or pause the service.

While the user logs on to the workstation the USB-Blocker PLUS starts:

- The program determines the groups which already exist locally or in the network
- It determines the groups, the logged on user is a member of
- It additionally stores the information in files
- It controls if the devices, which are connected to or installed on the workstations, should be monitored and if the user is allowed to use them.
- Optionally it blocks user's screen until the unauthorized device is removed or the blocking is released by administrator.

## 1.2 How secure is the USB-Blocker PLUS?

All components that are needed for the USB-Blocker PLUS are indeed visible for the default user but not changeable. The Service USB-Blocker, the user USBAdmin as well as the files in the installation folder belongs to these components.

We generally advise against assigning administrator rights to the user. These rights include a number of possibilities to deactivate or evade software. A standard user has no possibility to avoid the monitoring function of the USB-Blocker PLUS.

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

## 2 Program installation

### 2.1 System requirements

The USB-Blocker PLUS can be installed for the following operating systems (OS):

Windows 2000 Professional  
 Windows XP Professional//Home \*<sup>1</sup>  
 Windows 2000 Server  
 Windows 2003

For administration of groups the following systems can be used:  
 Active Directory (AD)

<sup>1</sup> For Windows XP see capture 3.1.6

Novell Directory (NDS)  
Local Windows groups

General: 20 MB of free space during the installation

**Note: Windows NT is not supported.**

## 2.2 Installing the USB-Blocker PLUS

The download package includes the files USB-Blocker\_PLUS.exe, USB-Blocker\_PLUS.msi und isscript8.msi. The MSI packages serve for the software distribution (chapter 4). The InstallShield Skript-Engine must only be distributed, if the installation via USB-Blocker PLUS.msi package produces an accordant error in the application protocol of the target system.

**The USB-Blocker works without server component. The installation on a server is not compulsively necessary. Only the configuration GUI has to be installed on an administrator workstation.**

In order to install the USB-Blocker PLUS, please start USB-Blocker PLUS.exe, choose 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 that you have already received from Institut für System-Management GmbH by default e-mail. You can install the program as a 30 days trial version for testing purposes.

For USB-Blocker PLUS configuration, the USB-Blocker Admin program is available for you. For installation, please choose the appropriate option.

### USB-Blocker PLUS Setup

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

#### Note:

The Service USB-Blocker is started when finalizing the installation. If there are already existing groups for monitoring management on the computer or in network (domain), the access management is activated immediately.

## 2.3 Uninstalling the USB-Blocker

The program can be uninstalled by using the Windows service program called Software.

1. Click on **Start** to open the Software service program, click on **System administration** and then click on **Software**.
2. Choose the program USB-Blocker PLUS from the list of installed programs and click on **Uninstall**.
3. Follow the instructions of the program.

## 3 Program Handling

The program handling is quite simple and contains three steps.

### 1. Creating groups

For every device, every class, service etc. that should be monitored, a group with appropriate description on a computer or in a domain has to be created. As soon as this group exists, the USB-Blocker PLUS allows the needed access only for members of this group.

### 2. Administering memberships

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

### 3. Configuring the USB-Blocker PLUS

The method of working of the USB-Blocker service can be changed by various configurations. For this purpose serve: assigning of users for group inquiry, group prefix defining, setting-up the log activity, NDS support activation and configuration.

## 3.1 Creating groups

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

### 3.1.1 Deliberations

The following deliberations are important:

1. Every device can be assigned to various groups.
2. To lock a device, at least **one** of these groups has to be available.  
**! The only existence of one of these groups leads to a device lock.**
3. To enable the usage of a monitored device to a user, the user has to be a member of at least **one** of these groups.
4. Groups can be applicable only for one device or they can be overlapping, applicable for more devices.
5. To every connected device will be assigned five properties by the USB-Blocker PLUS.

1. device service
2. device class
3. device class description
4. device name
5. device ID
6. To secure the unique identification of devices, these properties can be combined.
7. Due to Wildcards it is possible that different USB sticks of one chip set producer can be released in only one group. In order to phrase the Wildcards “asterisk” and “question mark” combinations of figures can be defined.
8. Internal devices are deactivated by the USB-Blocker PLUS. Herewith it has to be noted, that the device ID of apparently independent system devices can be identical. This can lead to an unintended device locking. It is recommendable no to lock via the device ID but via device classes and/or device services.

**Please, pay attention that the locking of internal hardware components can possibly lead to a breakdown of the system. Therefore please test your setting first on a computer that is offline.**

Except of this, there is a possibility to create two special groups.

1. HW\_TRUSTED
  - Members of this group can use all devices without restrictions.
  - The only existence of this group does not have any effect.
2. HW\_NOTRUSTED
  - All devices without exception are locked for members of this group. The usage of devices has to be allowed explicitly.
  - Member of this group, which are also a member of the group System-HardwareLock, applied for the appropriate system, are not able to change the hardware on this PC.
  - The only existence of this group has no effect.
  - Note:
    - ! ALL devices that means in this case really ALL!**
    - This does not affect 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, you can lock all USB mass storages globally by creating a group and then enable particular USB mass storages by using special device groups.

### 3.1.2 Group names ascertaining

The **USB-Blocker Admin** is available for ascertaining the required group names

→ Launch the USB-Blocker Admin program.

1. In order to open USB-Blocker Admin click on **Start**, click on **All Programs**, select the **USB-Blocker PLUS** entry and then click on the **USB-Blocker Admin**.

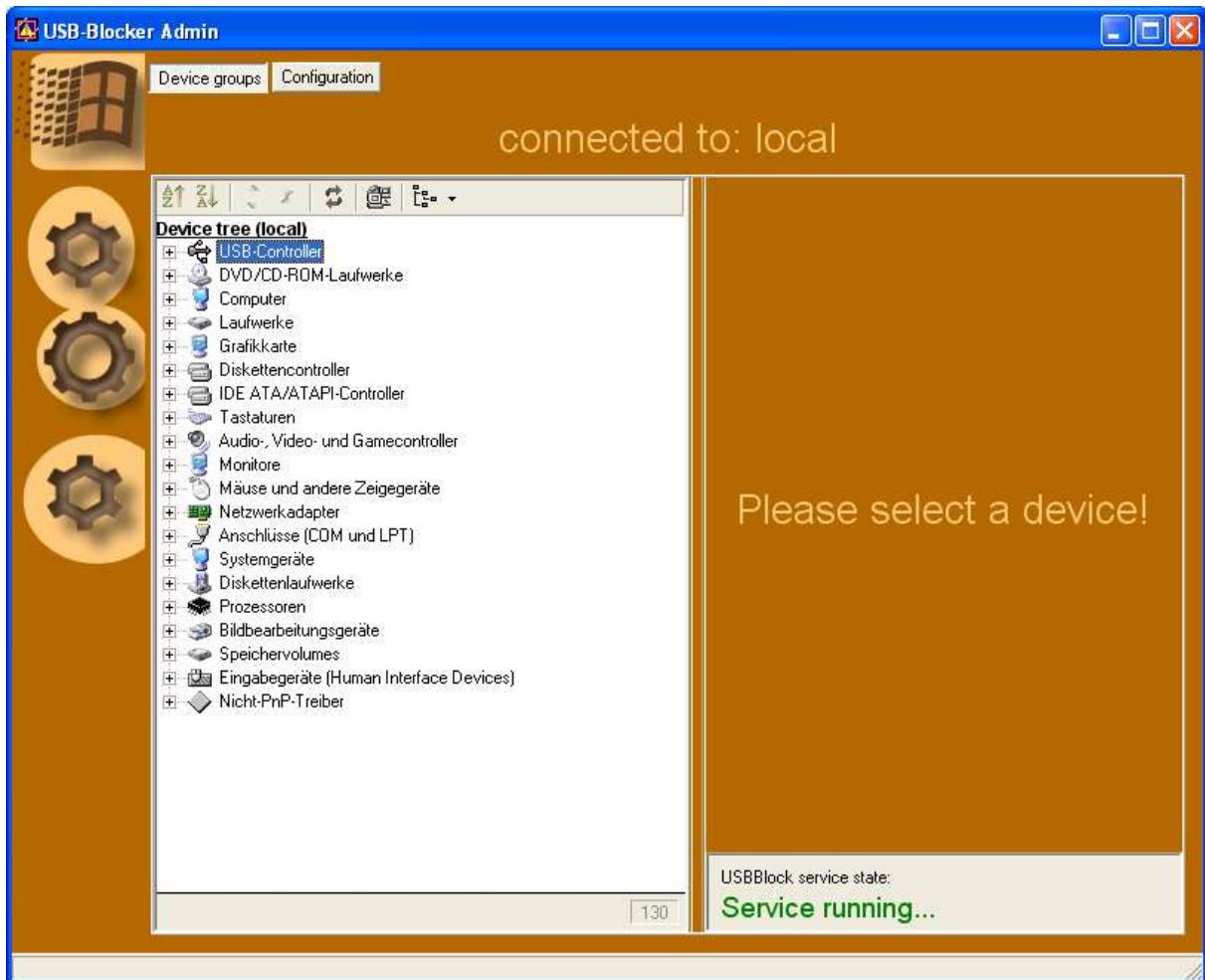


Figure 1 USB-Blocker Admin

In the left part of the program user interface is shown the device structure of the installed and connected devices of your computer. It is appropriate to the Windows Device Manager.

Using the symbol bar, you are able to:

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

The view of locally available devices is refreshed automatically by every hardware change. If you have established a remote connection to a computer, you have to refresh the view manually.

→ Connect the devices that you want to monitor to your computer or establish a remote connection to a computer to which the device is connected.

→ Find every device in the structure that you want to ascertain a group name for.

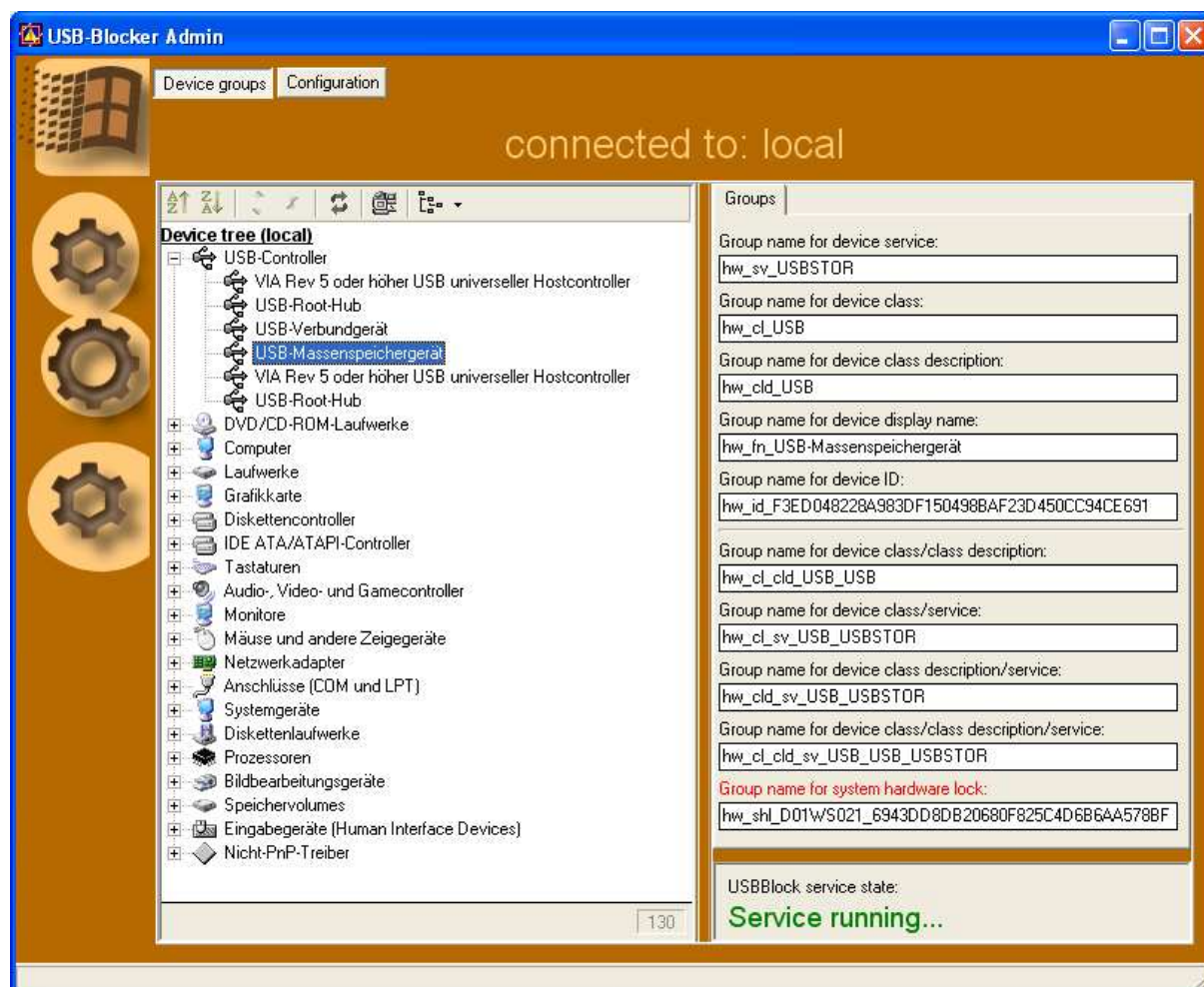


Figure 2 Detailed view of devices

In the detailed view on the right side the possible group names are displayed.

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

1. Device service
2. Device class
3. Device class description
4. Device name
5. Device ID

The further four group names are combined from these properties.

Example: An USB flash drive is listed:

1. as an USB mass storage below USB Controller
2. as <shown name> below Drives
3. as a standard volume below Drive volumes

To keep this context clear, switch the structure view and click on **Show devices by connections**.



Figure 3 Devices sorted by connection

As a matter of principle, every entry is a separate device and can be locked. Devices depended on these are also affected by the locking, so it could be possible that you have enabled dependent devices.

Select the group name that is the most appropriate to your locking strategy.

### 3.1.3 NEW: Restrict writing rights

From version 4.x of the USB-Blocker the writing access on data media can be restricted. If a device can be write-protected, it will be displayed by the checkbox **“Write protection groups”**.

If this option is activated, the displayed group names will be added by suffix **01**. This suffix describes that no data can be stored (written) on the accordant device. Reading access is still possible.

For members of a write protected group the write protect is abolished.

If there are any questions concerning migration from 3.x to 4.0, please take note of the chapter *FAQ!*

### 3.1.4 Naming conventions

The group names are usually shown with a prefix in USB-Blocker Admin. For the individual properties these are:

- |                             |         |
|-----------------------------|---------|
| 1. Device service           | hw_sv_  |
| 2. Device class             | hw_cl_  |
| 3. Device class description | hw_cld_ |
| 4. Device name              | hw_fn_  |
| 5. Device ID                | hw_id_  |

To the combinations of group names, the prefixes are also combined appropriately.

These prefixes are elective and should ease the group management. You can customize these prefixes in the USBBlock.ini according to your needs.

### 3.1.5 Administering memberships

The allowance for using the hardware devices is being administrated by membership in the local or domain group. In order to grant access for this user, he has to become a member of this local or domain group.

You have to be logged-in as **Administrator** or as a member of the **Administrators** group to be able to realize these tasks.

The proceeding is exemplarily described under using the computer administration in XP Professional. In several operating systems there are a number of administration and command line programs; by using them you can solve this task. See also the help to the appropriate operating system.

#### 3.1.5.1 How to set up a local group

1. Open **Computer Administration**.
2. Find **Groups** in the console structure.
  - Computer administration
    - System programs
      - Local users and groups
        - Groups
3. Click on **Action** and then click 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 Computer administration, click on **Start** and then click on **System administration**. 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 blanks as well as the special characters # , + " \ < > ;
- A group name cannot be built only of dots (.) or blanks (spaces).

### 3.1.5.2 How to remove a local group

1. Open **Computer administration**.
2. Find **Groups** in the console structure.
  - Computer administration
  - System programs
  - Local users and groups
  - Groups
3. Click with the right mouse-button on the group that should be deleted and then click on **Delete**.

### 3.1.5.3 How to add a member to a group

1. Open **Computer administration**.
2. Find **Groups** in the console structure.
  - Computer administration
  - System programs
  - 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 from 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 that 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**.

### 3.1.5.4 How to remove a member from a group

1. Open **Computer administration**.
2. Find **Groups** in the console structure.
  - Computer administration
  - System programs
  - 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. Choose the user or group in the **Members** field and then click on **Remove**.

### 3.1.6 Windows XP Home Edition

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

Check the existing local groups:

```
net localgroup
```

Apply a USB-Blocker device group:

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

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

```
net localgroup usb-blocker-group user name/group /add
```

Check the members of the USB-Blocker device group:

```
net localgroup usb-blocker-group
```

## 3.2 Configuring the USB-Blocker

It can be switched between the view for group- ascertainment and service configuration in the USB-Blocker Admin. After starting the program the view for group- ascertainment is by default. **For Purposes of configuration the program has to be started with local administrative rights!**



Figure 4 Switching between program views

### 3.2.1 Settings for USB-Blocker Admin User

In this area, the local Windows user used by the USB-Blocker can be changed. This user is created during the installation process on the computer and is equipped with a random password. This user has administrative rights and it will be needed to remove them from system when locking devices. The user for the USB-Blocker PLUS can be changed. It has to be taken into account that also this user must have administrative rights. There can be used local or domain users. Changing of the Admin Users is optional. *It is recommended not to change these settings!*

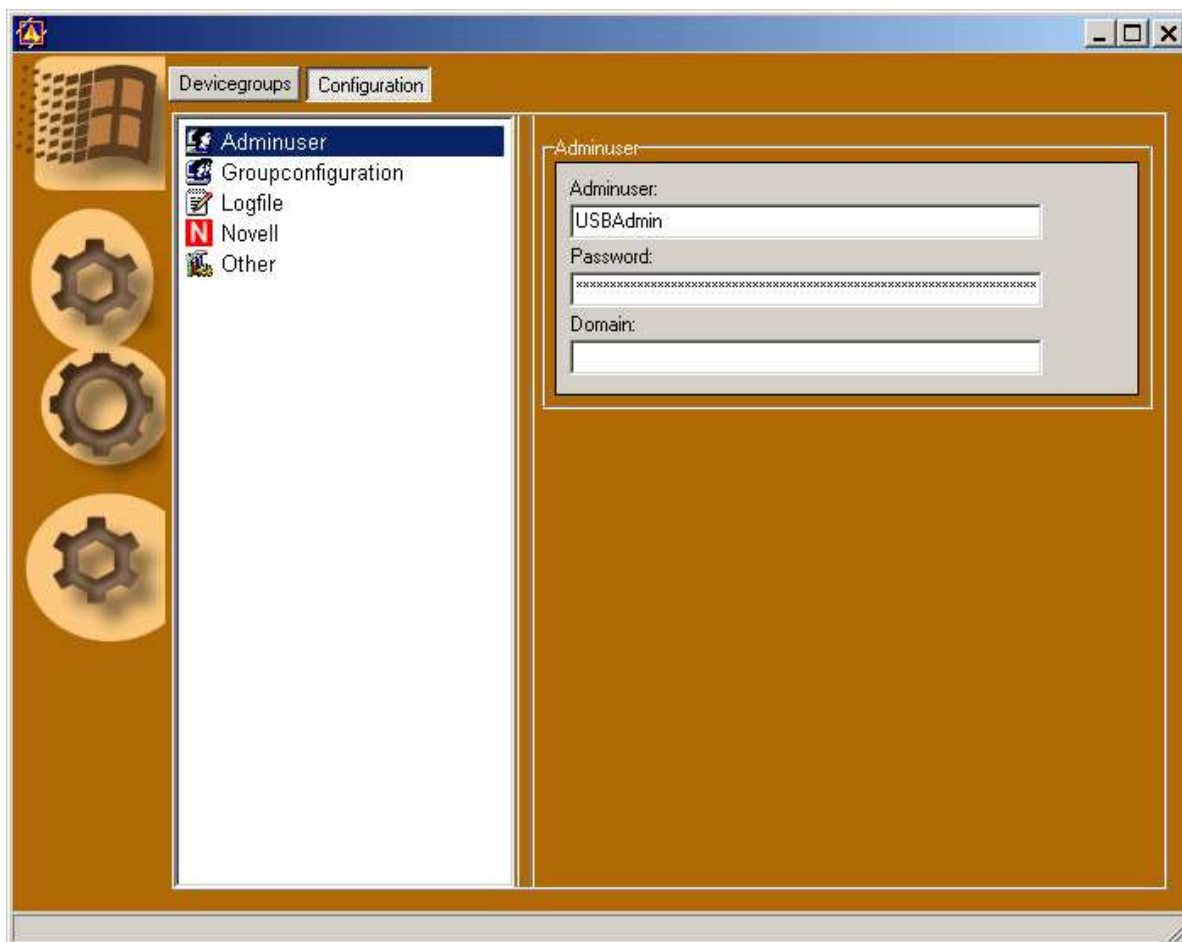


Figure 5 Settings for USB-Blocker Admin User

### 3.2.2 Settings for group configuration

All used groups for the USB-Blocker PLUS comply with an adjustable scheme. The best prefix is already pre-configured for all groups. These group prefixes can also be adjusted to own rules for groups in this part of USB-Blocker Admin. Changing of this setting is optional.

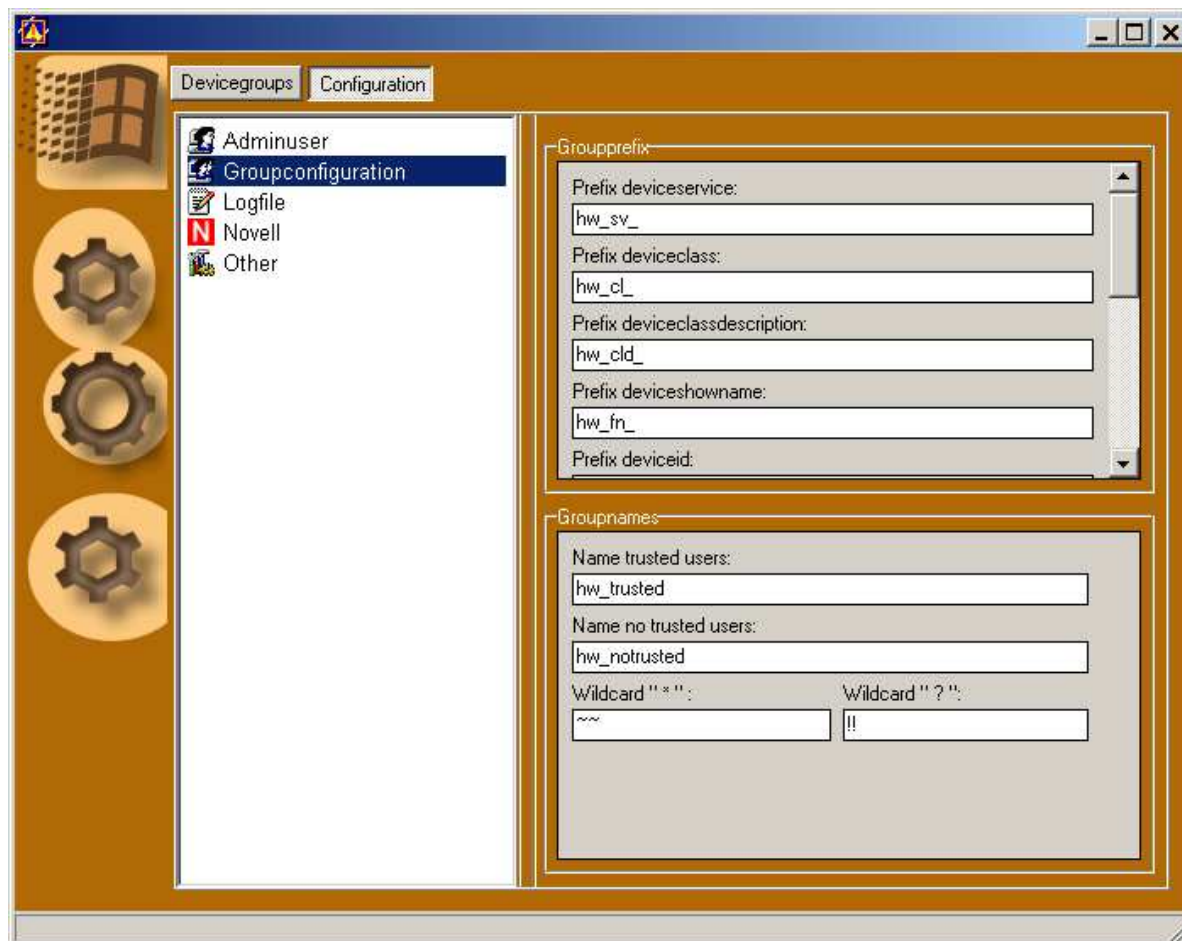


Figure 6 Settings for group configuration

### 3.2.3 Settings for log activity of the USB-Blocker PLUS

At this point of Admin Tool the log activity of the USB-Blocker can be configured. Default preset is the activation of the option with setting of the lowest level. There is the *Log Level* 1 up to 3. On level 1, there are only users and group data recorded which the USB-Blocker has recognized and which devices has been locked. Level 2 and 3 are for error analysis. These levels are set only after request by support, because there is a number of writing processes into the log file. The name and path of the log file can be configured. Changing of this setting is optional.

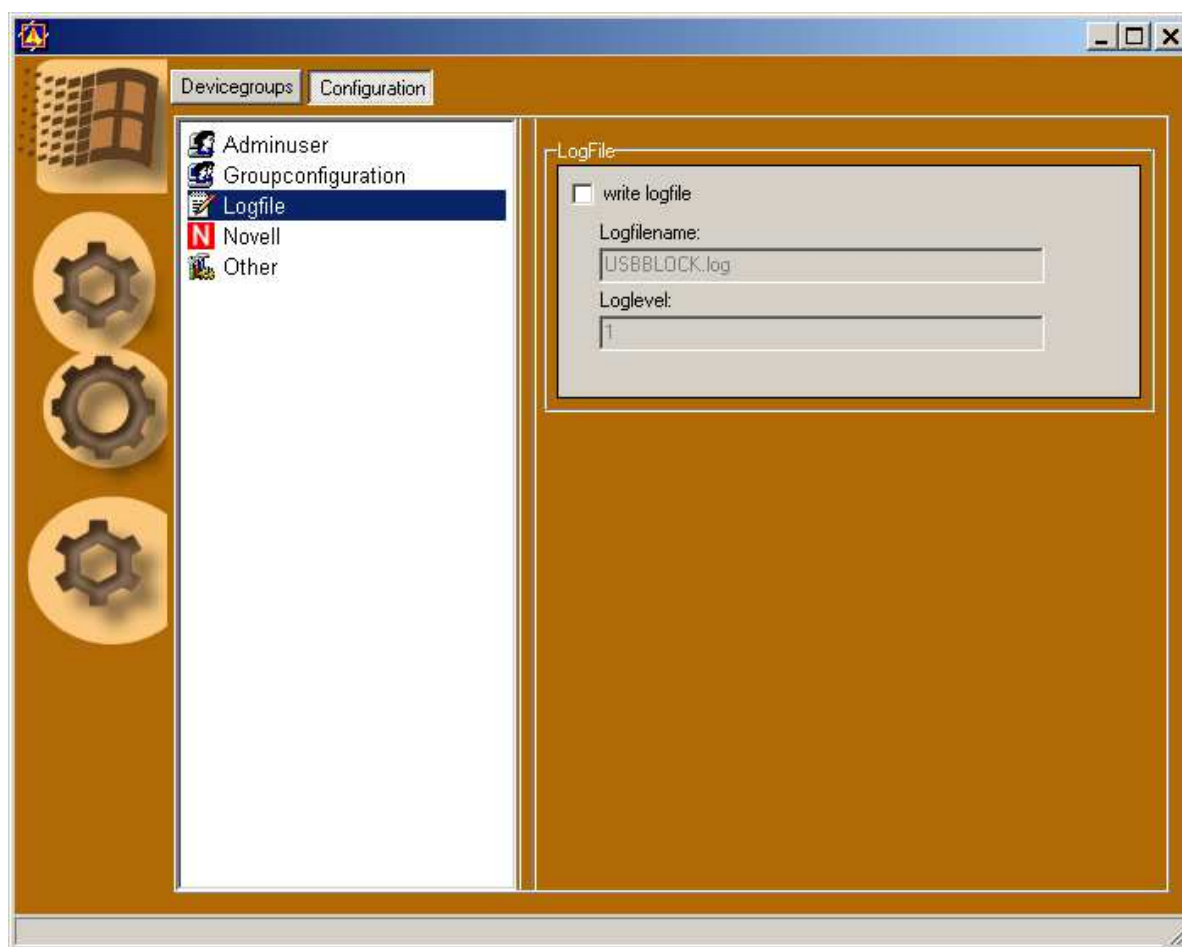


Figure 7 Settings for log activity

### 3.2.4 Settings for NDS Support

Settings represented in this view are necessary for proper cooperation of the USB-Blocker with NDS. After installing the USB-Blocker, the option “**use Novell**” is deactivated. This option has to be realized on all installed computers. The simplest possibility is to realize the setting on one computer and to distribute the key contained in the registry to other computers. After activating this option, the following input fields are available for following data:

a) **Use Admin User for the NDS connection (NDS)** – If the software distribution ZENworks is used, this option should be activated, because otherwise there can be problems by interacting with the ZENworks Client. By activating the option the admin user, defined by the USB-Blocker Admin, is used for building up the connection.

b) **Make group requests for this user account** – Here a user of the NDS has to be named, who has reading right for the whole organization and for all organizational units. This user serves for ascertaining the group configuration for the logging user. The USB Blocker Plus logs on to the NDS with this user and starts then the request operations.

Please pay attention, if one and the same NDS user has been named for all workstations, it is not allowed that this user is logged on several workstations at the same time.

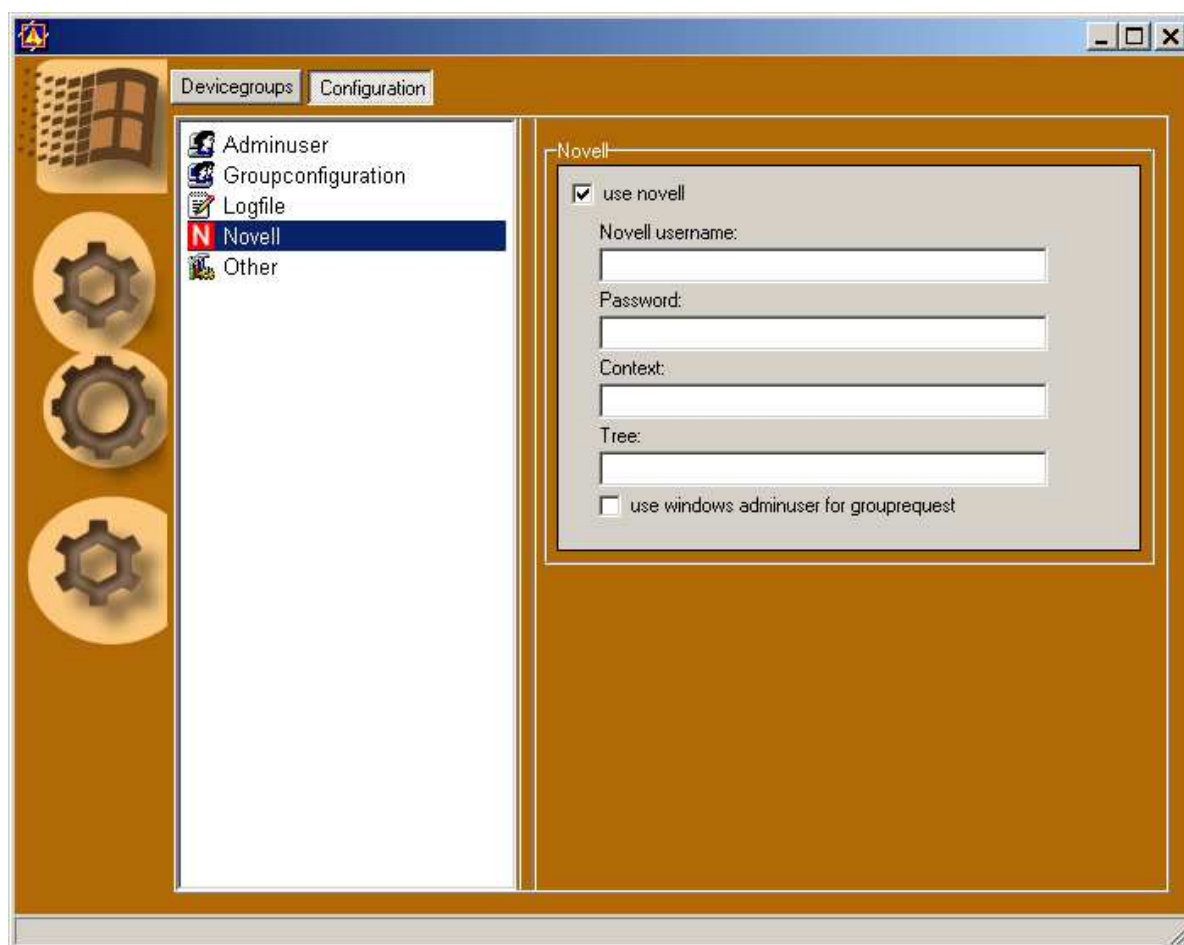


Figure 8 Settings for NDS/eDirectory Support

### 3.2.5 Settings for additional parameters

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

- a) **group refresh for device/disk change** means the 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 read-out again. The user does not need to log himself off and on when refreshing.
- b) The option **trust admin** deactivates the block function for users with administrative rights independent form the existing device group.
- c) The configuration point **Generate device ID from** is used for the setting of the generation algorithm of the device ID group. In seldom cases it happens that Windows assigned the same ID to different extern devices. In such case it is necessary to improve the identification process. The generation of the device ID group out of the iSerial number is preset. If this setting is not sufficient for a clear identification, you can create a more defined group via adding further device properties. At point 2 next to the iSerial number also the vendor ID and

- product ID is used for generating the device ID. At point 3 the device name is included additionally.
- d) Activate **use local hardware group**, if a locally applied device groups should be considered. It is recommended, to deactivate this option while using AD or Novell.
  - e) By clicking the **Groupfilter user** optionally the browser procedure in the first level of the directory service (ADS/NDS) for ascertaining the group can be shortened. By activating this option the group memberships of the configured user are used as blocking group. If the **Groupfilter user** is not member of this group, it cannot be used for blocking. The option using the Groupfilter user is enabled for NDS as long as the usage of NDS is not configured (3.2.4). You can find further description concerning use of filter user in chapter 7. The usage of this option is recommended emphatically.
  - f) The option **Display lock screen** activates the lock screen, which appear as long as the unauthorized device will be removed.
  - g) By clicking the button **Export Config** you can export the current configuration into a reg-file, which is required for software distribution.

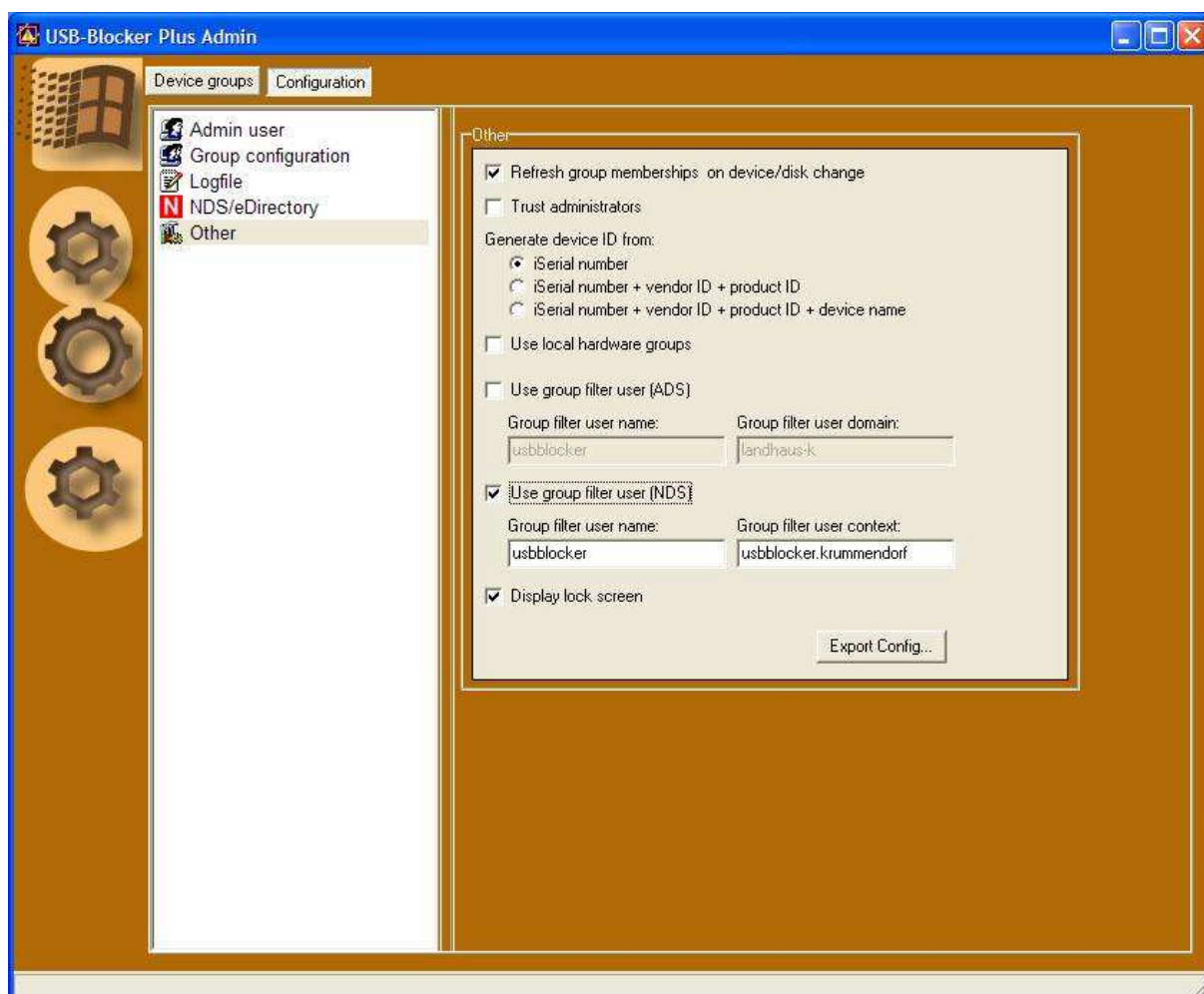


Figure 9 Settings for additional parameters

### 3.3 Group administration in NDS

After activating the option to connect the USB-Blocker PLUS to NDS and completion described in the point 3.2.4, the USB-Blocker PLUS reads out the appropriate user groups in the NDS. If the Groupfilter User should not be used, it is described in the following which versions of affiliations of users within the groups are possible.

#### 3.3.1 Possible group constellations

The USB-Blocker PLUS can evaluate groups and users that are directly underneath the organization and in OU's during an activated NDS connection. The following constellations of memberships are possible:

1. The user is applied directly in the organization.
  - a) The user is a member of a group that was applied directly in the organization as well.
  - b) The user is a member of a group that is not located in the OU.
2. The user has been applied in an OU.
  - a) The user is a member of a group that was also applied directly in the organisation as well.
  - b) The user is a member of a group that is located in the same OU as the user.
  - c) The user is a member of a group that is located in another OU as the user.

#### 3.3.2 Configuration hints for the NDS usage

It is recommended to install the USB-Blocker Admin on one computer from that 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:**

Concerning the administrative Novell user (described in 3.2.4) you have to pay attention to the following: Therewith the USB-Blocker PLUS with the user specified before can make competing (simultaneous) requirements for groups in NDS, there should be no login restrictions for this user.

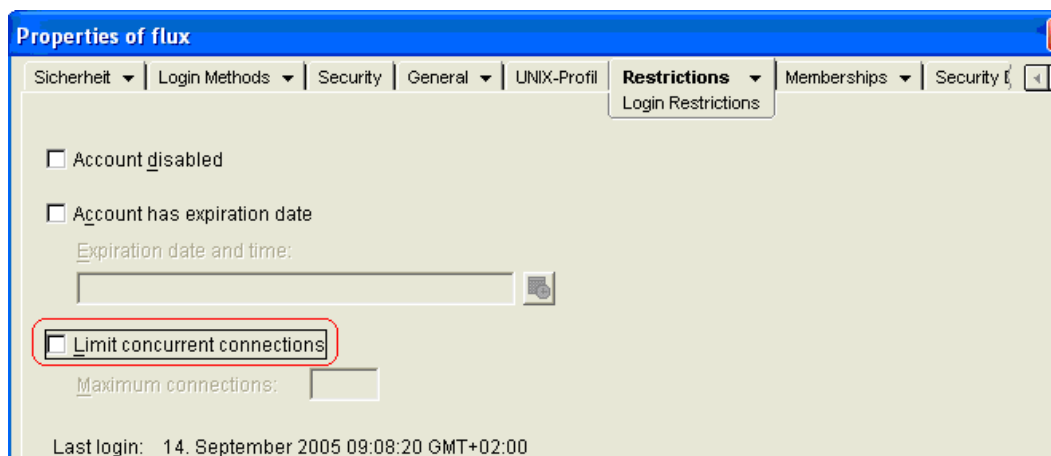


Figure 10 Settings for the administrative NDS user

## 4 Installation via software distribution

In order to ease the installation in network the USB-Blocker PLUS can be distributed to the client-workstations via systems for software distribution.

The vendor iSM GmbH provides a MSI file that is distributable by software distribution of Windows 2000/2003 domain as well as a MST file and their license files. The installation of InstallShield Skript Engine 8 is only necessary, if the installation on the clients fails with an accordant fault message in the application protocol.

The configuration file usblock.reg (3.2.5) exported by means of USB-Blocker Admin is transferred to the client via software distribution as well. For that purpose this file has to be stored in the same folder like the MSI file which has to be distributed. Then it is used for installation automatically.

## 5 Administration of USB-Blocker via group policies (GPO)

After installation of the administration panel there is an ADM-file in the installation directory of the USB-Blocker. This file can be integrated in GPO. In this way it is possible to change the configuration of the USB-Blocker on the clients comfortably.

For this purpose copy the ADM-file in the directory C:\Windows\inf of the domain controller. Open the GPO editor and create a new GPO.

Open the GPO and click with the right mouse button on administrative submittals in the category computer configuration. Select "add/remove submittal" and add the USB-Blocker ADM as submittal.

Whereas the policy settings of the USB-Blocker cannot be administered completely, the accordant filter has to be deactivated.

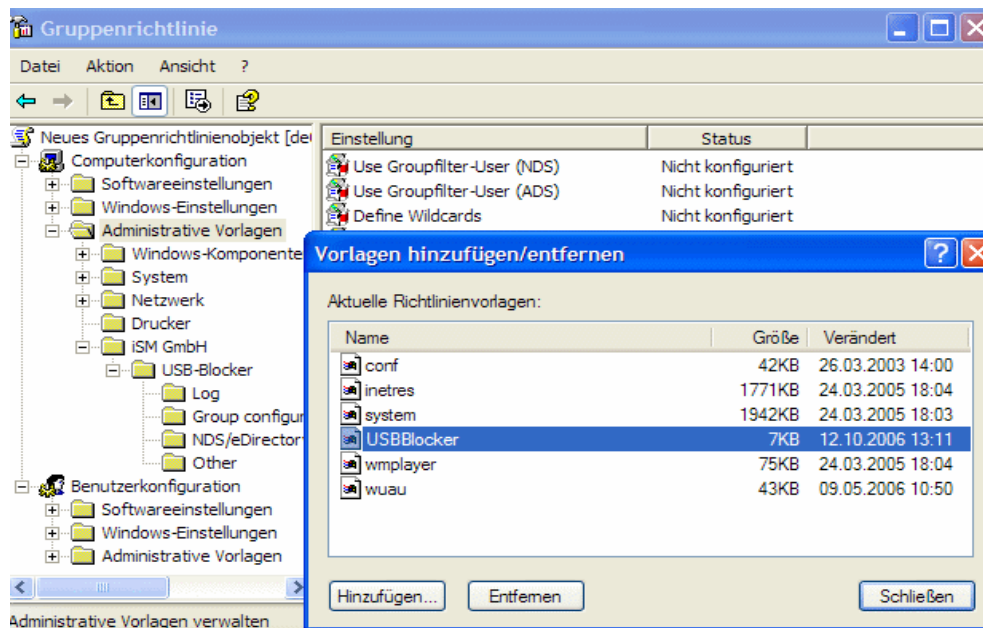


Figure 11 filtering policy settings

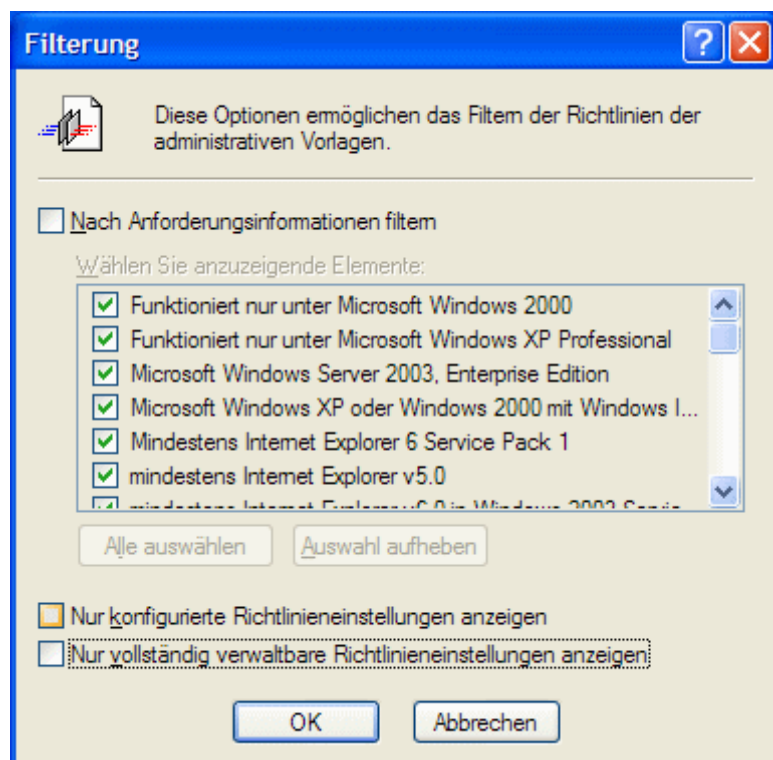


Figure 12 filtering policy settings

## 6 USB-Blocker PLUS 30 Days Trial Version

You can use USB-Blocker PLUS during the trial phase for 30 days without any restrictions.

During every start of the service USB-Blocker, there appears an 'About' window for 120 seconds. This window can be closed every time. It will also be shown during every start of the USB-Blocker Admin. Close it by clicking on the **Close** button.

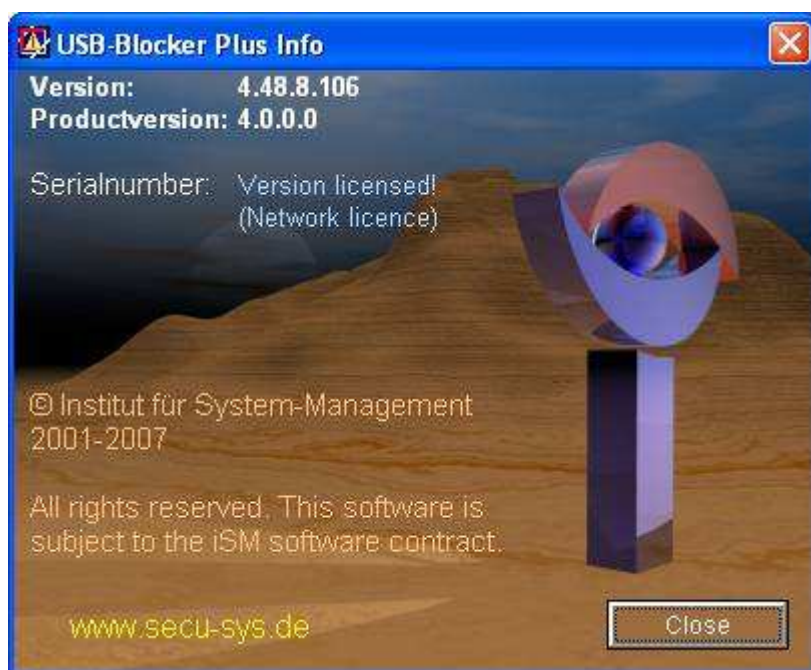


Figure 13 'About' window

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.

From this moment, all users can use the workstation without restrictions. An examination concerning the membership in the defined groups is not realized anymore.

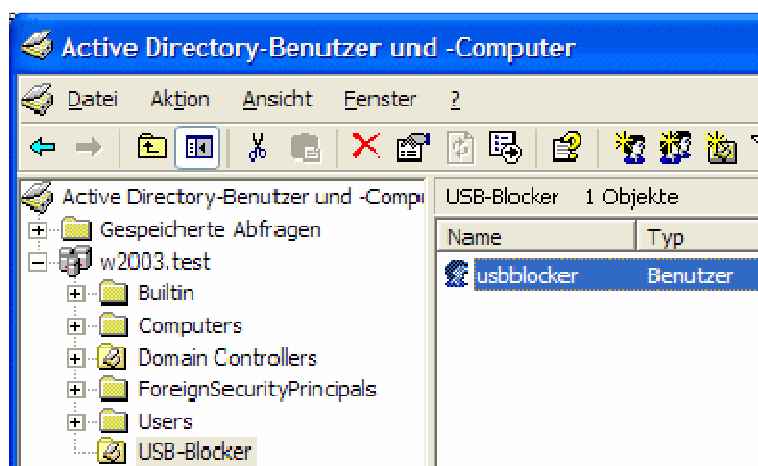
## 7 Example of configuration

Intention of this example configuration is the deactivating of all USB-mass storage media. USB devices, which are no mass storage media, will function further on. Additionally a special USB-stick should be allowed for use. Please reset non mentioned settings for the exemplary configuration to the default data.

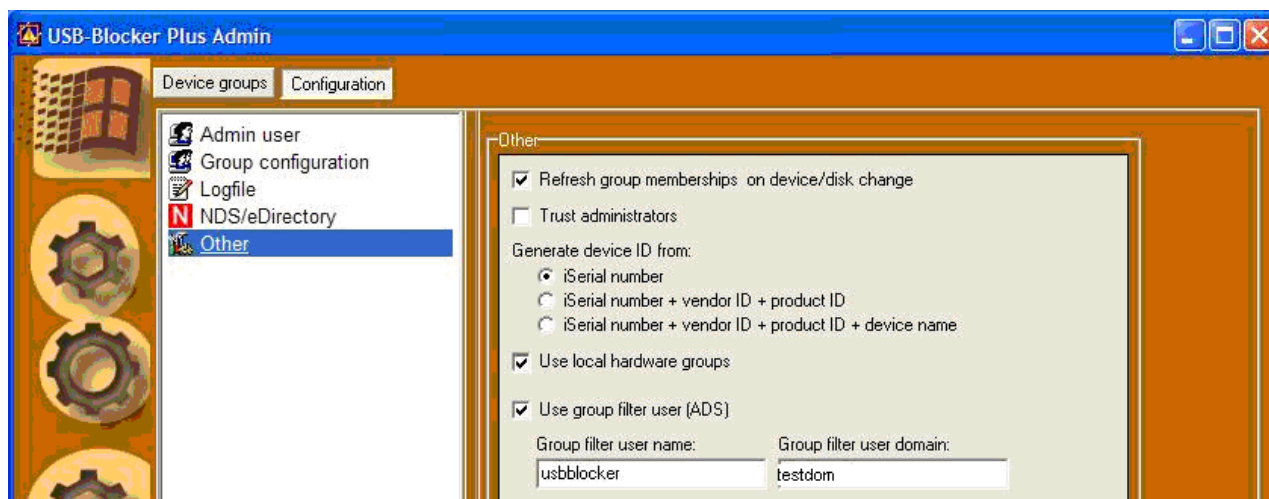
It is preconditioned that the USB-Blocker Admin is installed on the testing workstation and that e.g. a USB stick can be plugged and is operational. Furthermore write access to the Active Directory/ eDirectory is necessary. In order to realize the following steps the USB-Blocker Admin needs local admin rights.

### 7.1 Active Directory

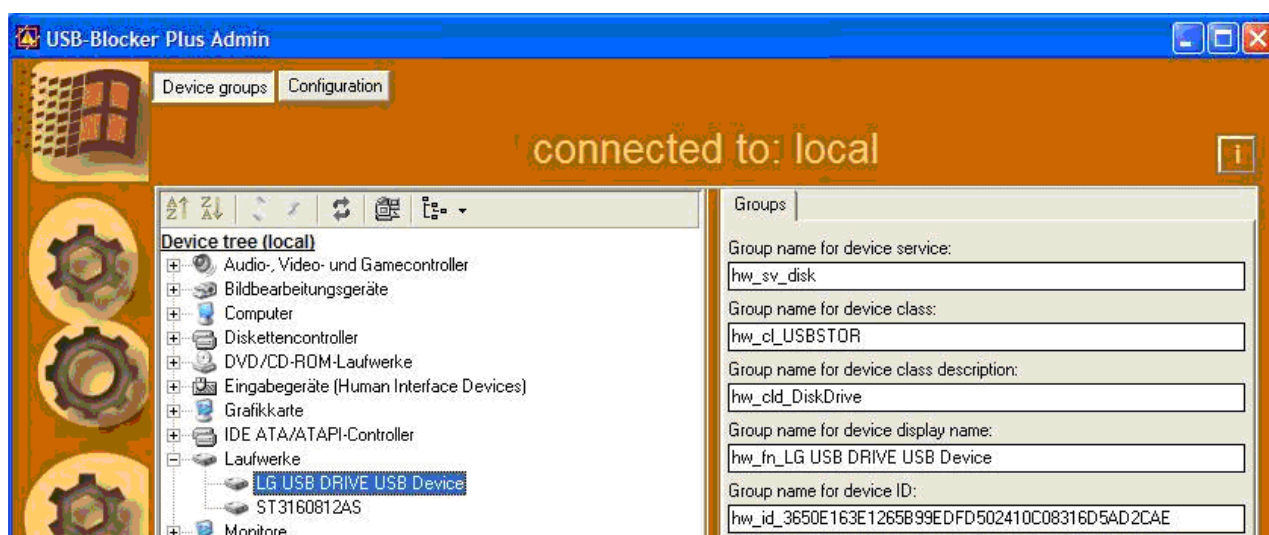
1. Open the console **Active Directory user and computer**.
2. Create a new OU e.g. named "USB-Blocker".
3. Create in this OU a new user e.g. usbblocker. Deactivate the **Kontooption** the user has to change the password for the next logon and activate the option **password never expires**.



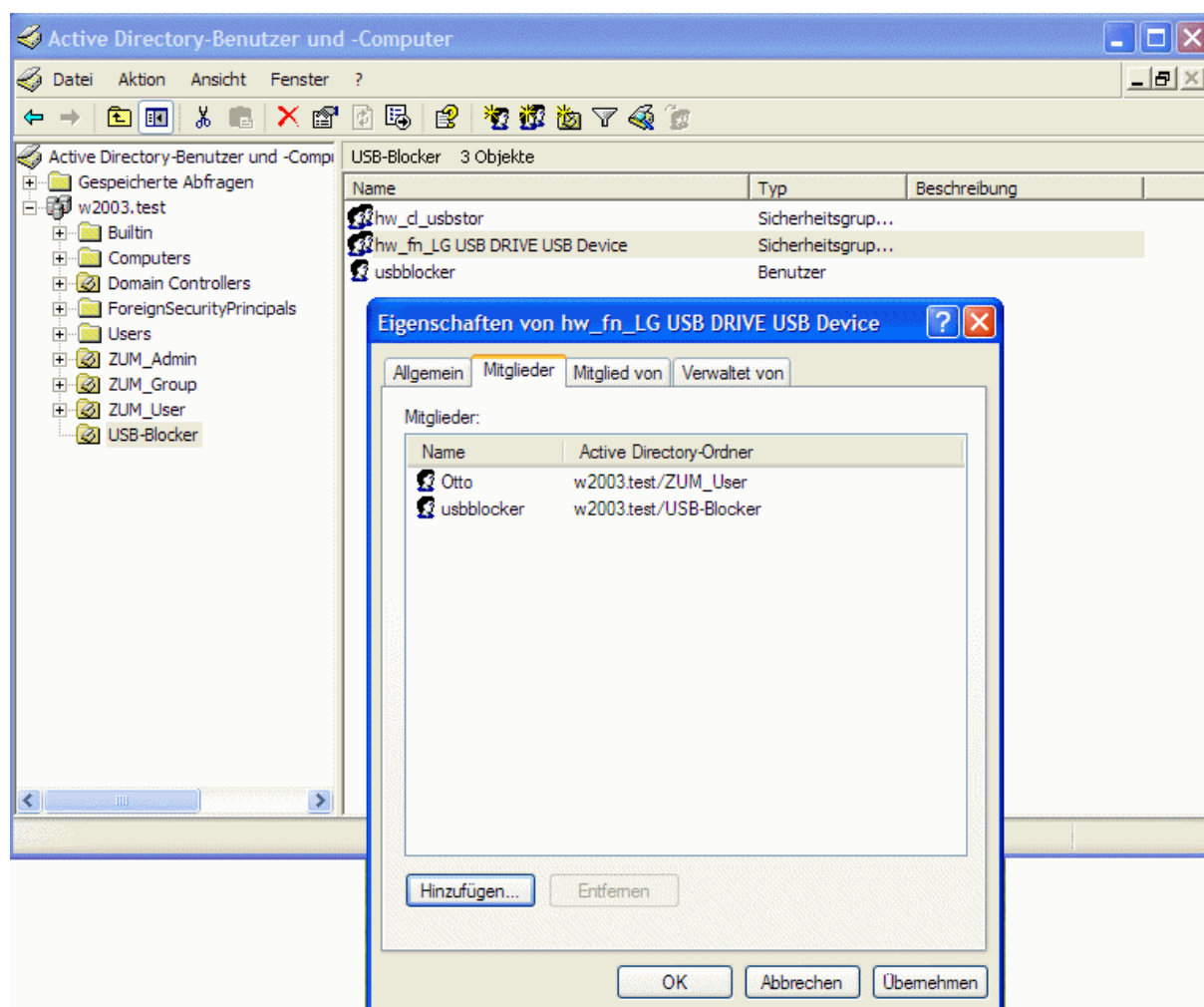
4. Keep the console opened and start the USB-Blocker Admin via Start menu.
5. Change the view to the configuration view by clicking the button **Configuration**.
6. Click on **Other Configurations**.
7. Activate the option **Use Groupfilter User (ADS)**.
8. Enter the user "usbblocker" applied before and the domain in the boxes.



9. Change to the device tree view of the USB-Blocker Admin by clicking the button **Device Groups**.
10. Click on the knot drive assemblies (Windows XP) or data media (Windows 2000).
11. Click on the USB stick, which you would like to release for use.
12. Copy on the right side „group name for device class” hw\_cl\_usbstor



13. Change to the console “Active Directory user and computer” and create a group hw\_cl\_usbstor in the OU of USB-Blocker. Global and universal groups of the type security are supported.
14. Change to the USB-Blocker Admin and copy on the right side “device name” for Example: hw\_fn\_LG USB DRIVE USB Device
15. Create also a new group in the AD.
16. Afterwards admit the user “usbblocker”, created at the beginning, as a member in both groups.
17. Admit one user, who should get the right of use for the device, as a member only of the group “**Group name for device display name,**”



18. Restart the service USB-Blocker in order to read the authorization data.

**Result:** After restarting the service the USB-stick will be ejected, as far as the logged on user is no member of the group “**Group name for device display name**”. After logon as the user Otto, who is a member of the group “**Group name for device display name,**”, the USB-stick can be used again. A renew plugging of the stick is not necessary.

**Reason:** In the case described above a restrictive strategy is realized. 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 allowed to use the accordant device. In the example Otto became member the group “**Group name for device display name,**”. Therefore the he is allowed to use the device.

Generally:

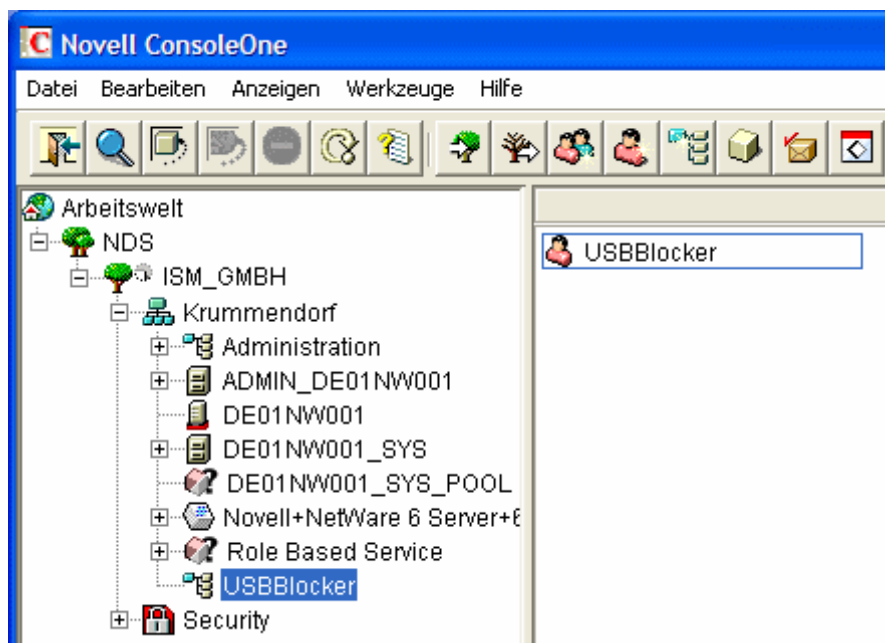
1. The group filter user must be member of all groups, which are relevant for USB-Blocker. This account should not be used for other purposes.
2. The membership in a group permits the use of the accordant device(s).

Note:

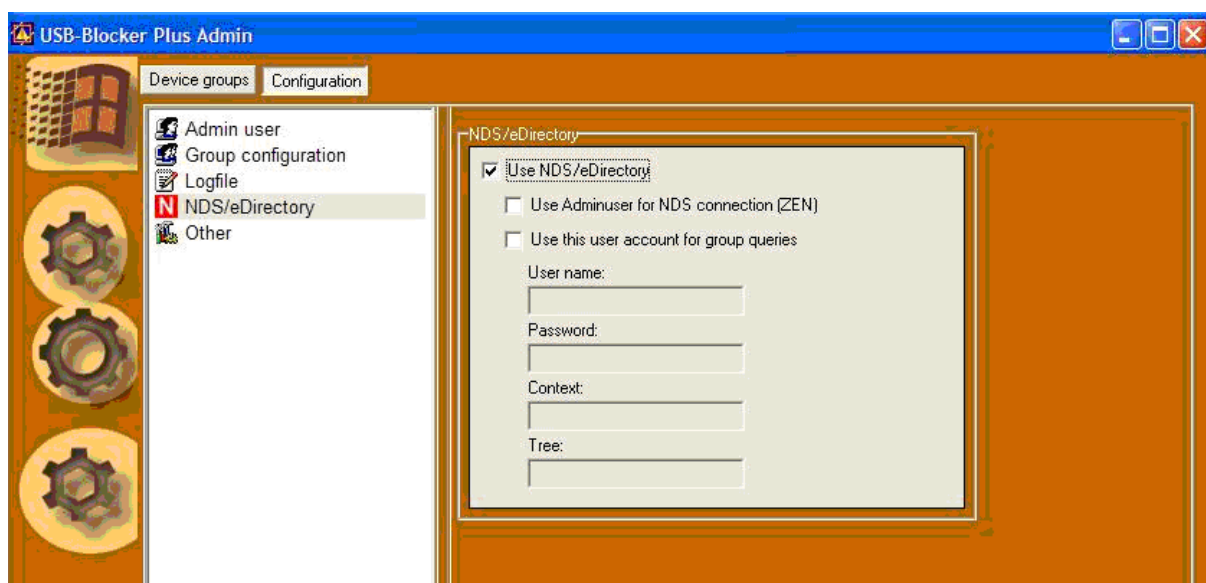
Group membership in the AD are effective not until new logon.

## 7.2 NDS/ eDirectory

1. Open the ConsoleOne and create a connection with the tree.
2. Create a new OU e.g. with the name "USB-Blocker"
3. Create a new user within this group e.g. usbblocker.

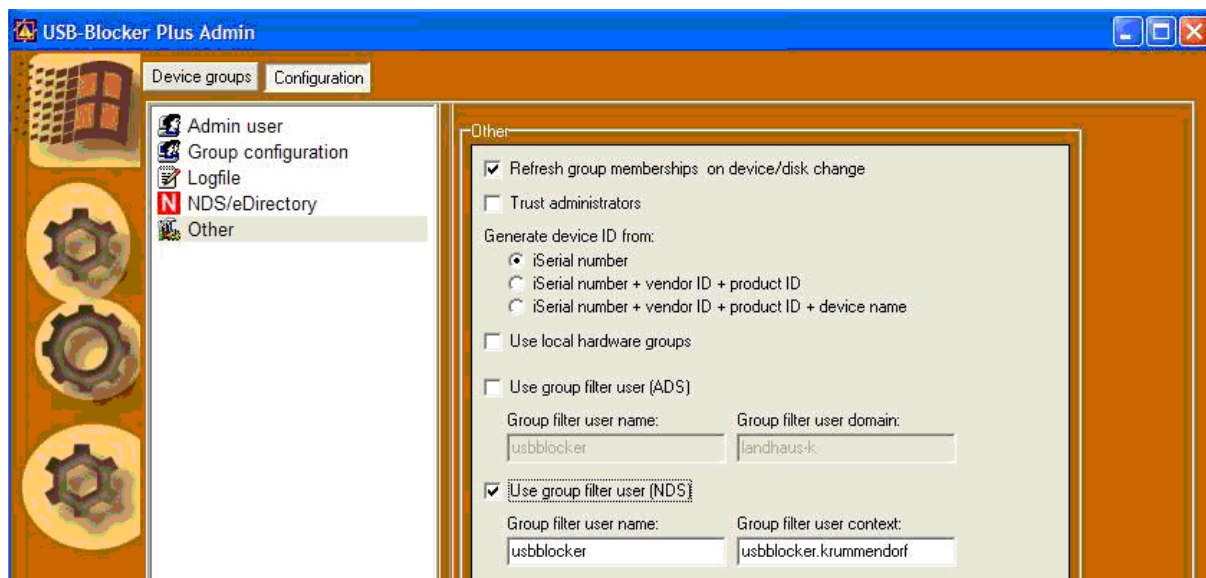


4. Keep the console opened and start the USB-Blocker Admin via Start menu.
5. Change the view to the configuration view by clicking the button **Configuration**
6. Click on NDS/eDirectory and activate the option "use NDS/edirectory".

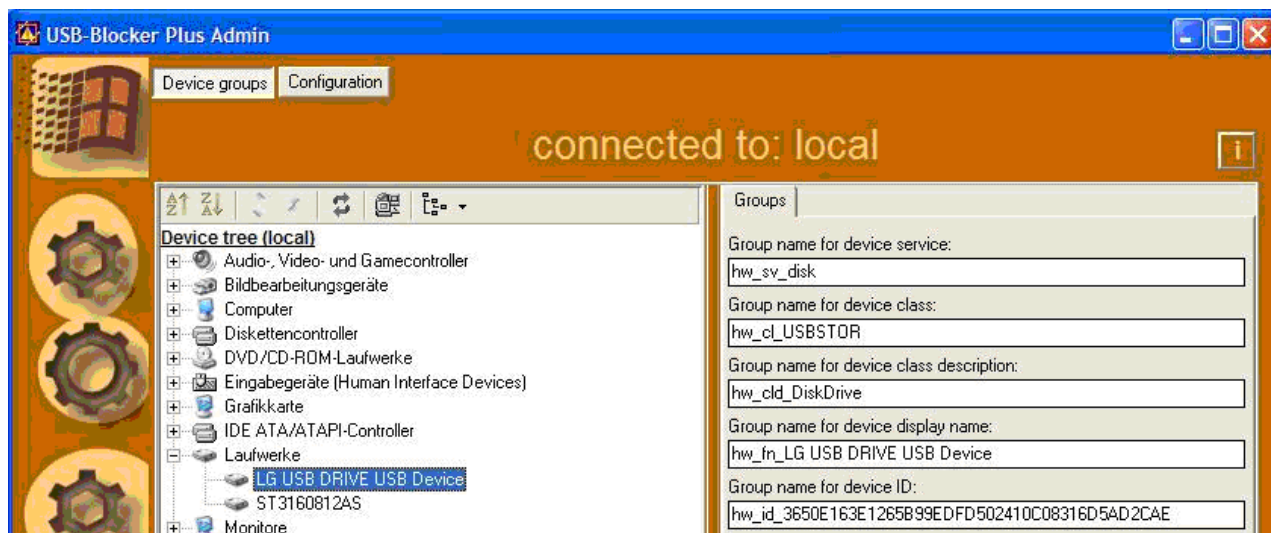


7. Change the configuration and click on "Other configurations"

8. Activate the option “use group filter user (NDS)”
9. Enter the user “usbblocker” applied before and his context (without tree) into the boxes.

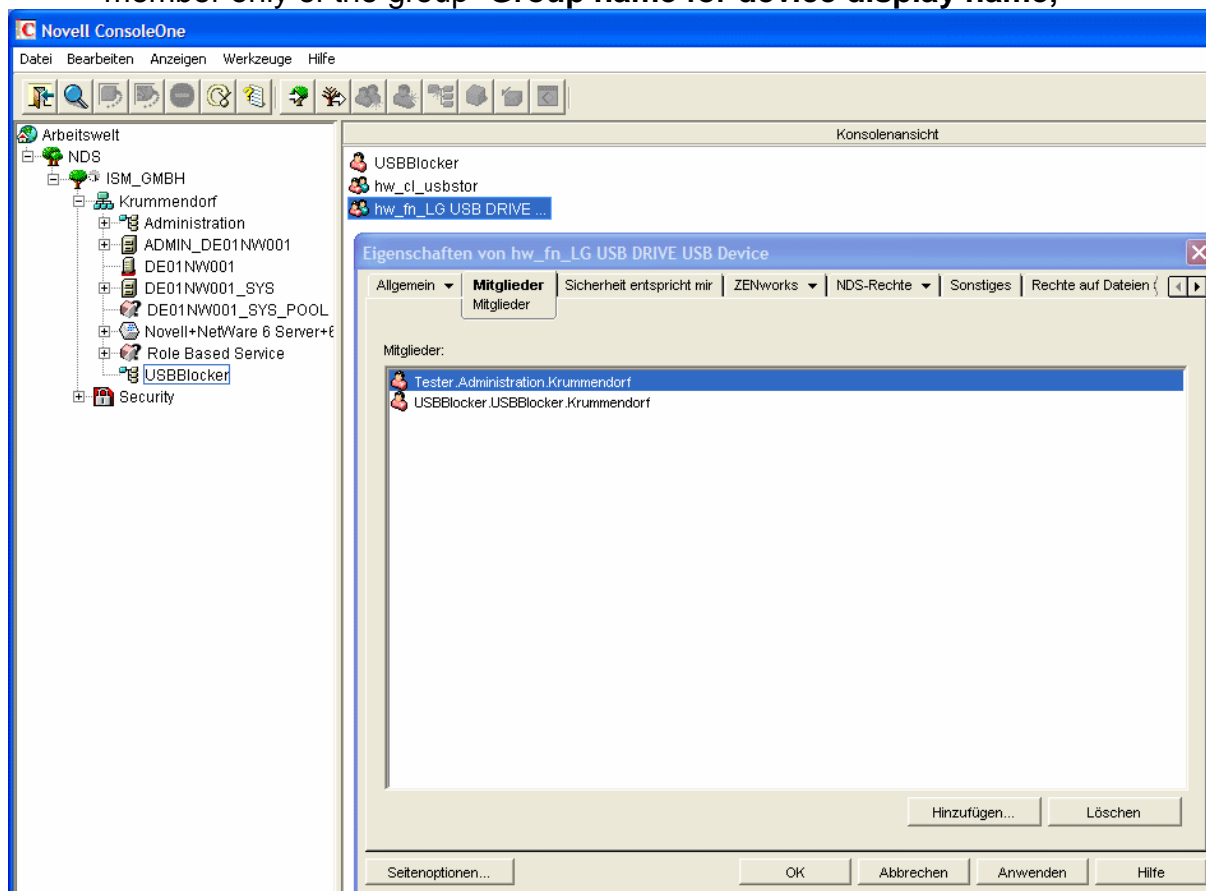


10. Change to the device tree view of the USB-Blocker Admin by clicking the button **Device Groups**.
11. Click on the knot drive assemblies (Windows XP) or data media (Windows 2000).
12. Click on the USB-Stick
13. Copy on the right side „group name for device class” hw\_cl\_usbstor.



14. Change to the ConsoleOne and create a group hw\_cl\_usbstor in the OU of the USB-Blocker.
15. Change to the USB-Blocker Admin and copy on the right side Group name for device display name, e.g. hw\_fn\_LG USB DRIVE USB Device
16. Create this group also in the NDS/eDirectory
17. Afterwards admit the user “usbblocker”, created at the beginning, as a member in both groups.

18. Admit one user, who should get the right of use for the device, as a member only of the group “**Group name for device display name,**”



**Result:** After restarting the service the USB-stick will be ejected, as far as the logged on user is no member of the group “**Group name for device display name**”.

After logon as the user, who is a member of the group “**Group name for device display name**”, the USB-stick can be used again. A renew plugging of the stick is not necessary.

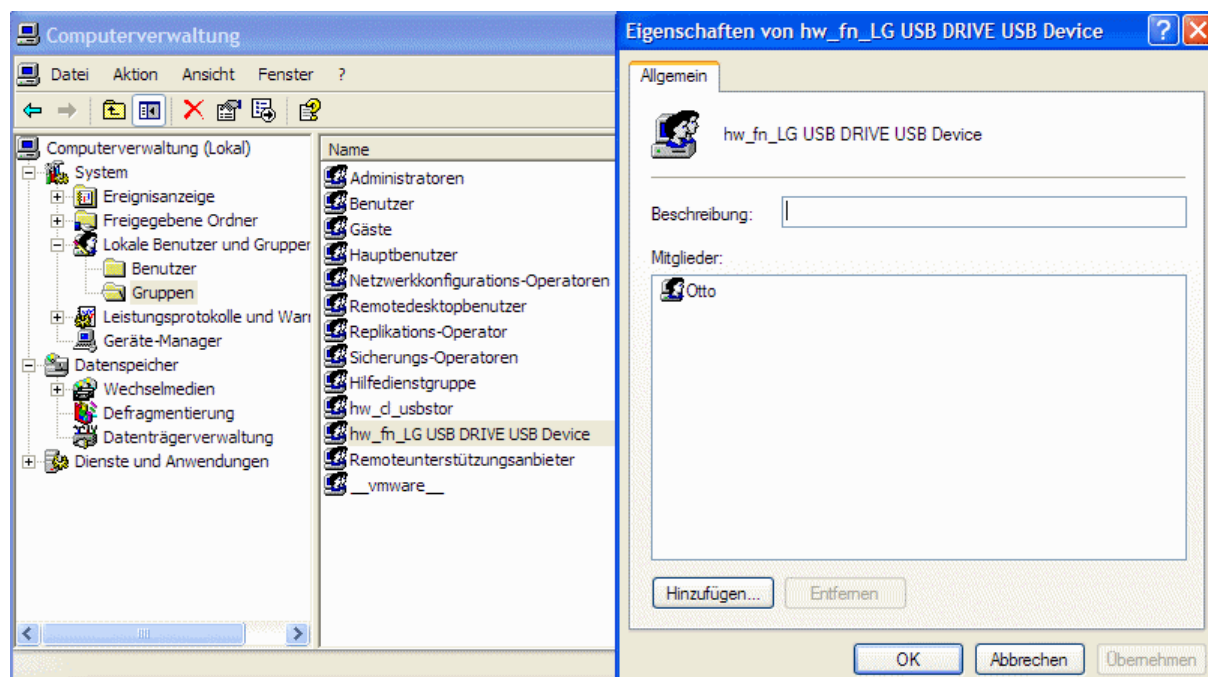
**Reason:** In the case described above a restrictive strategy is realized. Generally all USB-Mass-storage media are blocked, because of the group hw\_cl\_usbstor. If a user is a member of the group, he is allowed to use the accordant device. In the example *Tester* became member the group “**Group name for device display name**”. Therefore he is allowed to use the device.

Generally:

1. The group filter user must be member of all groups, which are relevant for USB-Blocker. This account should not be used for other purposes.
2. The membership in a group permits the use of the accordant device(s).

## 7.3 Local

1. Open the USB-Blocker Admin via Start menu.
2. Click on the knot drive assemblies (Windows XP) or data media (Windows 2000).
3. Click on the USB-stick
4. Copy on the right side „group name for device class” hw\_cl\_usbstor.
5. Open the local Computer Administration and copy on the right side
6. Change to the USB-Blocker Admin and copy on the right side **Group name for device display name**, e.g. hw\_fn\_LG USB DRIVE USB Device
7. Create also this group with the computer console locally.
8. Admit one user, who should get the right of use for the device, as a member only of the group “**Group name for device display name**,”



9. Restart the service “USB-Blocker” in order to read the authorization data.

**Result:** After restarting the service the USB-stick will be ejected, as far as the logged on user is no member of the group “**Group name for device display name**,”.

After logon as the user, who is a member of the group “**Group name for device display name**”, the USB-stick can be used again. A renew plugging of the stick is not necessary.

**Reason:** In the case described above a restrictive strategy is realized. 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 allowed to use the accordant device. In the example *Tester* became member the group “**Group name for device display name**”. Therefore he is allowed to use the device.

Generally:

The membership in one group permits the use of the accordant device(s).

## 7.4 Deactivate all USB devices

In order to deactivate all USB devices, there are two possibilities.

### 7.4.1 Deactivate all USB device classes

The following groups have to exist:

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

Afterwards the groups related to the devices can be created, in order to allow the use of certain devices. This procedure is recommended.

### 7.4.2 Deactivate the USB hub

The following groups have to exist:

<b>hw_cl_USB</b>	- Sperrt den USB HUB
------------------	----------------------

A user, who is allowed 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.

## 8 Important

**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.**

## 9 FAQ

1. Which group domain and type of group should be used for groups in the AD?
  - a. Global and universal groups with the type security are supported. This comes up to the Microsoft recommendations concerning group design AD.
2. Which Kontooptions must be activated for the group filter user?
  - a. Please secure, that the user do not has to change the password for the first logon. The password must not expire.
3. How must the .mst-file be used for distribution, therewith the USB-Blocker is installed with licence data on the clients?
  - a. In order to realize a uncontrolled installation and to use the .mst-file with licence data for the 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?
  - a. This is an intended procedure. The USB-Blocker only blocks the workstation as long as it is necessary to remove all blocked devices from the system. The text boxes on the lock screen down right are regularly not necessary. By entering the administrator's account into the text boxes the screen can be released, if one device cannot be removed.
5. How about the security in the safe mode?
  - a. The safe mode is not satisfying concerning the intention of the USB-Blocker. In this mode only some few system drivers and services are loaded. The USB-Blocker is not loaded. 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, in order to avoid a logon via domain account (on the supposition that the users do not know any local account). This can be achieved by renaming the key:  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network`  
 to e.g.  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Networkfalse.`
6. I applied a domain user as a member of a blocking group. Why can the released device not be used?
  - a. Changes within group memberships became first activated in a Windows domain after new logon
7. I use the USB-Blocker 3.x and would like integrate the write protection feature of version 4.x. What do I have to consider?
  - a. In order to protect a device against writing, you have to add a group with the same name add by the suffix 01 e.g.: hw\_cl\_usbstor\_01. If write protection should be effective for only some members of an existing device group, you have to apply these users as members of the write protection group. If needed it is recommended to rename the device group

## 10 Functional way of the USB-Blocker PLUS

The program is set-up as a Windows service and is started automatically by the Windows Operating System.

### Hint:

The service USB-Blocker guarantees the control of devices. Take into account that the user has no possibility to terminate the service.

The USB-Blocker PLUS is activated by user's logon.

- It ascertains the groups available locally or in network
- also the groups in that the logged-on user is a member.
- saves this information additionally to a file
- checks if the devices connected and installed on the computer should be monitored or can be used by the user.
- Locks the screen of the user until the unauthorised device is removed or until the lock is cancelled by administrator.