

USB - Blocker PLUS

PRODUCT
INFORMATION



USB-Blocker PLUS Management Summary

Internal data are ignored and/or neglected culpably by the employees for the annoyance of many administrators. Thus data are exchanged frequently for example by user friendly USB memory sticks, CD-ROM, DVD, floppy disk or external hard disk, without testing these devices for sensitive databases. Therefore enterprise networks are threatened by viruses in spite of using firewalls.

A further big danger is data theft via storage media. Employees influence unintentionally or wilfully the security of company networks by using several mass storage media.

By the USB-Blocker PLUS all devices managed by the Windows Device Manager e.g. the use of external (USB sticks) and internal (CD-ROM, disk drivers) storage media are regimented on all clients.

Benefits of the USB-Blockers PLUS:

- Facilitation of work in the IT risk management of enterprises
- Protection of all interfaces (USB port, PCMCIA, fire wire)
- Sustainability by building the USB-Blocker up to Windows Device Manager and regimentation of all listed devices
- Control of all external and internal storage media
- Access control by group membership
- Differentiation of individual devices or device groups possible
- ADS and NDS function

Economic effects:

- Mass storage media are no risk any more
- Prevention of data theft and protection of the enterprise network
- low costs and low integration and installation expenditure (additional server not necessary)

The USB-Blocker PLUS does not lock the entire USB port. The administrators are able to make different hardware components like printer or scanner available for the employee. Therewith the access can be allowed or denied specifically for individual users.

USB-Blocker PLUS Initial Situation

By application of storage media several risks are generated:

- unauthorised use of software (license offences)
- unauthorised access on data (data manipulation)
- unauthorised use and transfer of company internal data (privacy and company secrets)
- „import“ of viruses.

These risks enhance the pressure on the IT Management to increase the internal security of company networks.

Data theft or import of viruses by means of storage media have to be prevented. However, the functions and working procedures of business processes must not be influenced negatively.

In the first step of safeguarding the company networks by the USB-Blocker PLUS the use of all storage media can be forbidden. Normally it is not possible to disconnect the USB port in general, because several external (authorised) devices like scanner or printer must be still available.

In the second step the use of selected devices can be permitted selectively for the user.

By the use of USB-Blocker PLUS the access control affords configuration of the storage medium by means of access control mechanism in the Active Directory (ADS) or Novell Directory (NDS).

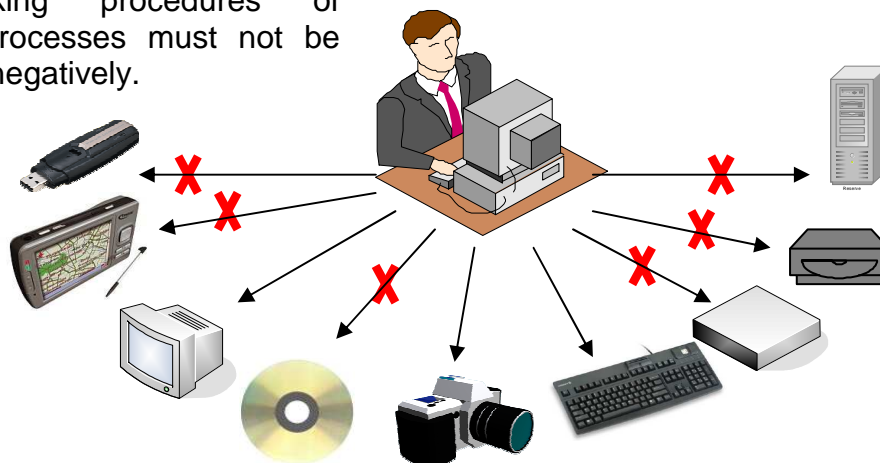


Fig. 1 The employee „Journalist“ is allowed to use the devices keyboard, screen and camera on his local workstation.

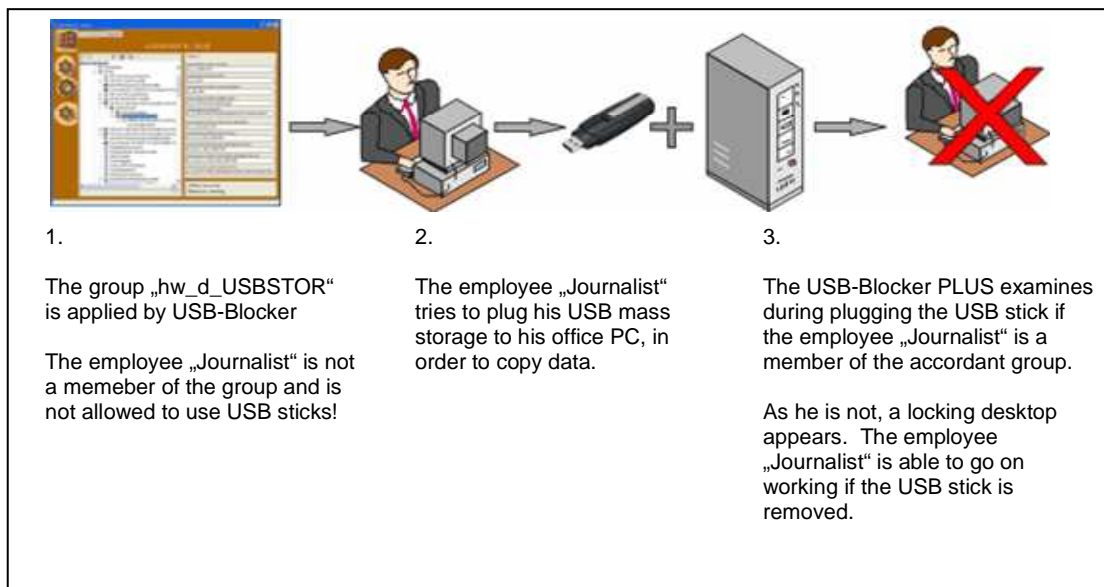
USB-Blocker PLUS Functionality

In the case of locking or authorisation of storage media to use there is a differentiation between device class, service affiliation, device ID and further properties. In order to guarantee a clear identification of devices, it is possible to combine these properties.

The USB-Blocker evaluates the different properties of the used devices. During the plugging process the USB-Blocker PLUS recognises these device properties and examines if there is a user group that belongs to the device type ascertained by Windows and if the applied user is a member of this group. (These groups can exist as well in ADS as in NDS.)

If there is no membership, the ejection mechanism of Windows is activated and a window informs the user about this process. During this process the pc is locked in order to prohibit that the user is able to influence this ejection process.

Internal devices like CD ROM and disk drives are not able to eject, of course. In this case an unauthorised use is stopped by deactivating internal devices via USB-Blocker PLUS.



USB-Blocker PLUS Active and Novell Directory Service

USB-Blocker PLUS and ADS

The application of USB-Blocker PLUS in networks with Active Directory enables an evaluation of local groups and groups in ADS. If a domain user registers to the pc all USB-Blocker PLUS relevant groups and user memberships in the ADS are required and buffered locally. This buffering is used for the maintenance of the blocking function in the case of a not existing domain-connection.

USB-Blocker PLUS and NDS

By the USB-Blocker's connection to the NDS a broad support of existing network infrastructures is possible. The configuration in NDS is done in the same way like in the ADS, via user groups, which enables a support of existing organisational structures in the NDS. The NDS function can be activated as an additional option.

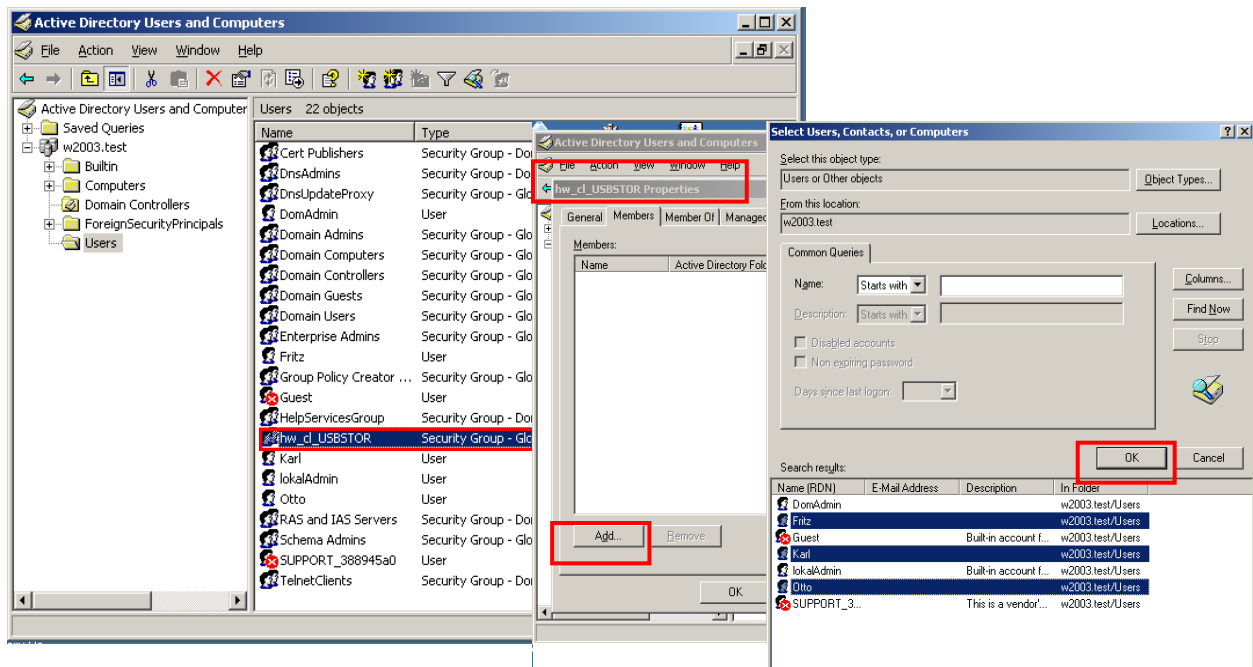


Fig. 2 Adding of users „Fritz“, „Karl“ and „Otto“ to the group hw_d_USBSTOR in the Active Directory. For these users the access to the USB port is allowed.

USB-Blocker PLUS Integrated in *bi-Cube*[®] IPM

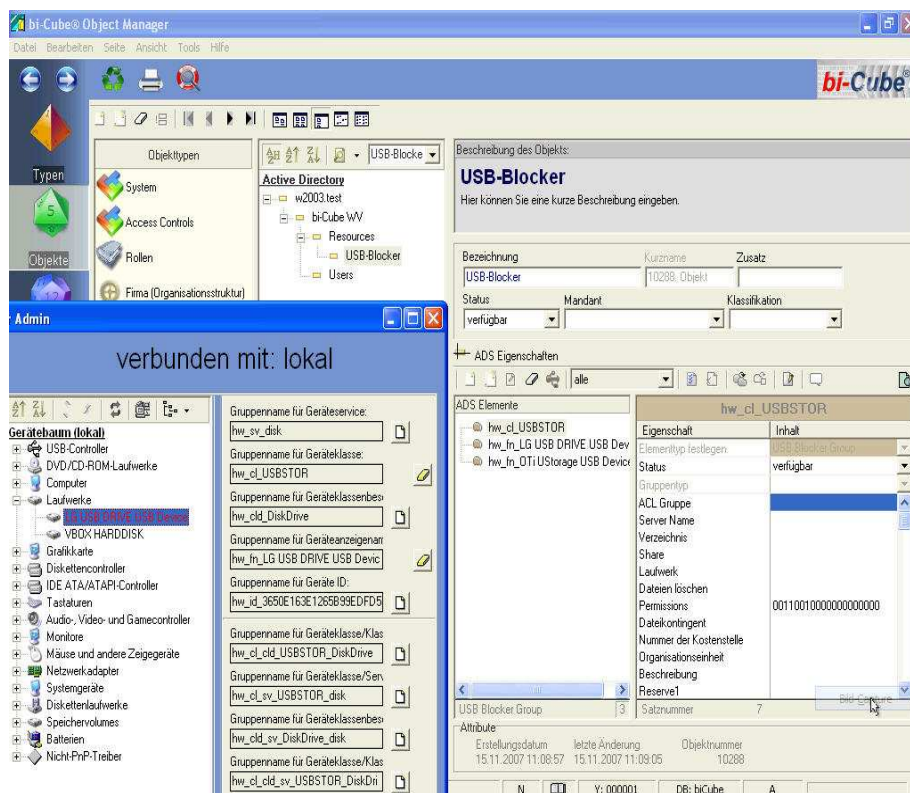
As integrated component in the developed solution of iSM's *bi-Cube*[®] IPM, it is also possible with the USB-Blocker PLUS, to process an automatically and rule based allocation of authorizations, for external and internal hardware, by roles.

Therefore, it is feasible with this matured role management to allocate authorization profiles, clear and structural. This is optimal for the setup and process organization in the enterprise.

The results are at high security standard and additionally a reduction of administration complexity.

The roles are centralized defined, and decentralized assigned to the employee, according to the competence, or job position.

The employee is automatically a member of a group in the active directory or 'Novell directory', and receives all, for him important, authorizations.



Protection against data theft and import of viruses

www.usb-blocker.com

USB-Blocker PLUS Integriert in **bi-Cube**® IPM

An additional advantage is the extensive **bi-Cube**®-based analysis and log function, in the new integrated USB-Blocker PLUS.

With the assistance of a log viewer, all local log files are analyzed. USB-Blocker events can be comfortably activated and analyzed by a web surface. Furthermore, it is

possible to export reports of the web surface into the known csv-format, or to send them through automatically generated e-mail.

Thus the connection of the USB-Blocker PLUS to the Identity & Provisioning Management **bi-Cube**®, offers a broad variety of functions for the administrator.

The image shows two overlapping windows. The background window is the 'bi-Cube IPM Web' interface, which includes a navigation menu (Service Center, Dokserver, SOP-Tools, Compliance), a language dropdown (Deutsch), and a user login section (y000001). The foreground window is the 'bi-Cube Configuration Manager' application, which displays a log viewer for the file 'C:\Programme\ISM\data\log\bi-cube'. The log viewer shows a table of events with columns for Typ, Datum, Uhrzeit, Quelle, and Meldung. The log entries include information about program accounts, LDAP binds, data file operations, and unauthorized device removal attempts.

Typ	Datum	Uhrzeit	Quelle	Meldung
Information	2007-09-19	16:03:28	ecdoc_dc	ProgramAccount : y020046
Information	2007-09-19	16:03:28	ecdoc_dc	ProgramAccount (impersonate/logon) : cor
Warnung	2007-09-19	16:04:03	ecdoc_dc	Bind : LDAP://contoso.com/RootDSE fail
Information	2007-09-19	16:04:03	ecdoc_dc	ADsSchema NO read
Information	2007-09-19	16:04:03	ecdoc_dc	DataFileOUT : contoso.com_20070912_1f
Information	2007-09-19	16:04:03	ecdoc_dc	DataFileERR : contoso.com_20070912_1f
Information	2007-09-19	16:04:03	ecdoc_dc	DataFileTMP : contoso.com_20070912_1f
Information	2007-09-19	16:04:03	ecdoc_dc	Exchange User : cn=y000004,ou=bi-cube,
Warnung	2007-09-19	16:04:24	ecdoc_dc	Bind : LDAP://contoso.com/RootDSE fail
Information	2007-09-19	16:04:24	ecdoc_dc	Loop
Information	2007-09-19	16:04:24	ecdoc_dc	Exchange User : cn=y000004,ou=bi-cube,
Warnung	2007-09-19	16:04:45	ecdoc_dc	Bind : LDAP://contoso.com/RootDSE fail
Information	2007-09-19	16:04:45	ecdoc_dc	Loop
Information	2007-09-19	16:04:45	ecdoc_dc	Loop
Information	2007-09-19	16:04:45	ecdoc_dc	data\N_CloseDataFile
Information	2007-09-19	16:04:45	ecdoc_dc	iso.DeleteFile - C:\Programme\ISM\data\o
Information	2007-09-19	16:04:45	ecdoc_dc	iso.MoveFile - C:\Programme\ISM\data\inq
Information	2007-09-19	16:04:45	ecdoc_dc	DataFileOUT : contoso.com_20070912_16
Information	2007-09-19	16:04:45	ecdoc_dc	iso.CopyFile iso - C:\Programme\ISM\data
Information	2007-09-19	16:04:45	ecdoc_dc	ProgramAccount : contoso.com\y020046
Information	2007-09-19	16:04:45	ecdoc_dc	ProgramAccount (impersonate/logoff) : y0C

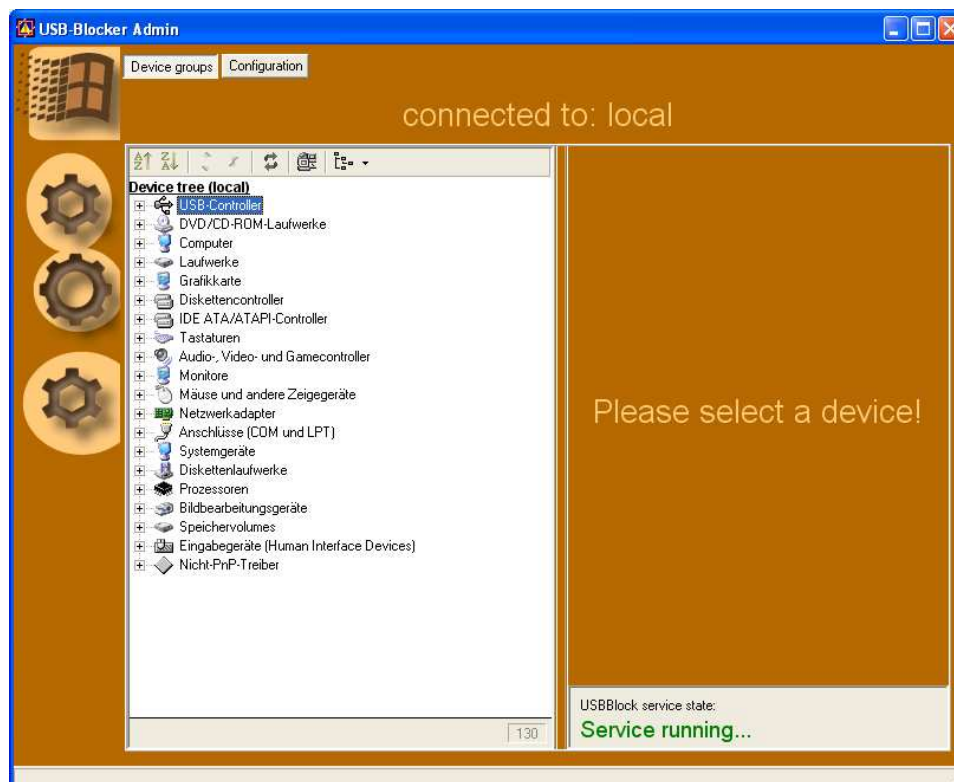
USB-Blocker PLUS Tool for analysis and configuration

USB-Block Admin

In order to realise the security function, it is necessary to be able to evaluate the device properties and their context.

Due to analysis intentions the iSM has developed the USB-Block Admin, which can make the required data available for the administrator. With the received data it is smoothly possible to generate the necessary groups on the local pc in ADS or NDS.

Furthermore this administration tool offers the possibility to do all program settings comfortably via only one surface. Compared to the configurations by means of setting files this surface is an improvement mainly concerning the administrator job, because the comfort is increased definitely.



USB-Blocker PLUS

Key Benefits

- By using the USB-Blocker PLUS there is no connection available, which enables use of not-released hardware components.
- The USB-Blocker PLUS controls every change in the Windows device Manager. The outcome of this is the sustainability, because even not yet known devices will be able to be ejected or to be deactivated in the future.
- By having an overview about storage media that are allowed to use the job of the IT management to secure the company's network is eased very much
- The USB-Blocker PLUS is a security tool, which protects next to the USB port also fire wire interfaces or PCMCIA ports against unauthorised access.
- Depending on the user that is logged on, the use of different ports is allowed or locked for the accordant devices. (selection)
- The USB-Blocker PLUS provides a broad support of existing network infrastructures because of the connection to ADS and NDS.
- Because of Wildcards in both operating systems it is possible to approve different devices of one and the same developer or vendor with only one group. In order to express the wildcards "starlet" or "question mark" character combinations can be defined at the USB-Blocker PLUS.

USB-Blocker PLUS System Requirements

The USB-Blocker PLUS can be installed on the following systems:

- Windows 2000
- Windows XP
- Windows 2000 Server
- Windows 2003

For administering the groups the following systems can be used:

- Active Directory (ADS)
- NovellDirectory (NDS)
- NT4
- local Windows groups

20 MB of free space during the installation

Installation type:

Demo version:

Setup with optional language (German or English).

License version:

Individual setup for every customer. Building of MSI and MST packets for network distribution.



iSM –Institut für System-Management GmbH

Oldendorfer Str.12

18147 Rostock

Germany

Tel. +49 (0)381 37 57 3-0

Fax +49 (0)381 37 57 3-29

E-Mail: info@secu-sys.de

Web: www.secu-sys.com

© Copyright Institut für System-Management

Information about iSM products is subject to the updating utility. They can deviate independently of it in insignificant points of the functionality of the current versions in the sense of the advancement of the products. In this document mentioned names about persons and/or enterprises or other objects are to be understood than fictitious examples, as far as it is not differently proven.

The reproduction or transmission of this document for any purposes (also in part) is permitted in principle only with written permission of the iSM.