

Product Information

bi-Cube[®] USB – Blocker

Technologies Solutions Trends Experience

Table of contents

1	MANAGEMENT SUMMARY	3
2	AUSGANGSSITUATION.....	4
3	FUNKTIONALITÄT.....	5
4	ACTIVE UND NOVELL DIRECTORY SERVICE	6
5	ANALYSE- UND KONFIGURATIONSWERKZEUG.....	7
6	INTEGRIERT IN <i>BI-CUBE[®]</i> IPM	8
7	KEY BENEFITS.....	10
8	SYSTEMVORAUSSETZUNGEN (OHNE <i>BI-CUBE[®]</i> INTEGRATION).....	11

1 Management Summary

Upsetting to the administrators, company internal data security policies are often ignored and neglected by employees. Via user friendly USB memory sticks, CD-ROM, DVD, floppy disks or external hard disks, data is exchanged without testing these devices of sensitive data records. Thus, enterprise networks could be infected by viruses in spite of using firewalls.

Another great threat is the data theft via storage media. Employees influence unintentionally or wilfully the security of company networks by using several mass storage media.

With the **bi-Cube[®] USB-Blocker** all devices managed by the Device Manager, the use of external (USB memory sticks) and internal (CD-ROM, disk drivers) storage media are regimented on all clients.

Benefits of the **bi-Cube[®] USB-Blocker**:

- Facilitation of jobs in company's IT risk management
- Protection of all interfaces (USB port, PCMCIA, fire wire)
- Sustainability by setting up the **bi-Cube[®] USB-Blocker** to the Device Manager and the regimentation of all listed devices
- Control of all external and internal storage media
- Access control by group membership
- Possible differentiation of individual devices or device groups
- ADS and NDS function

Economic effects:

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

The **bi-Cube[®] USB-Blocker** does not lock the entire port. Different hardware components like printer or scanner remain available for the employees by the administrators. Thus, the access by individual users can be permitted or denied.

2 Initial Situation

By using storage media, several risks may arise:

- unauthorised use of software (license violation)
- unauthorised data access (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.

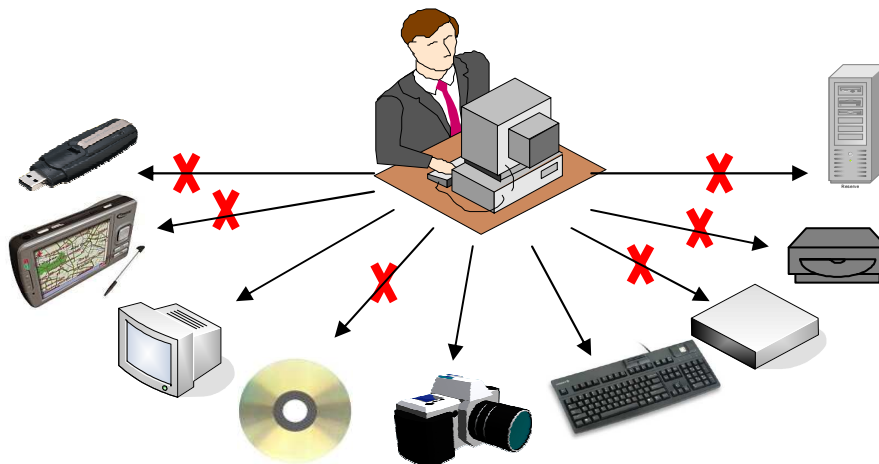
Data theft or import of viruses by means of storage media have to be prevented. However, the functions and procedures of

business processes must not be influenced negatively.

In the first step of safeguarding the company networks, the use of all storage media can be forbidden with the **bi-Cube[®] USB-Blocker**. Usually it is not possible to disconnect the USB port, because several external (authorized) devices like scanner or printer must still be available.

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

With the **bi-Cube[®] USB-Blocker** the access protection takes place by the configuration of the storage medium, supported by general access protection mechanisms in the Active Directory or Novell Directory.



Picture 1: The employee "Journalist" is permitted to use the device keyboard, monitor and camera on his local workstation.

3 Functionality

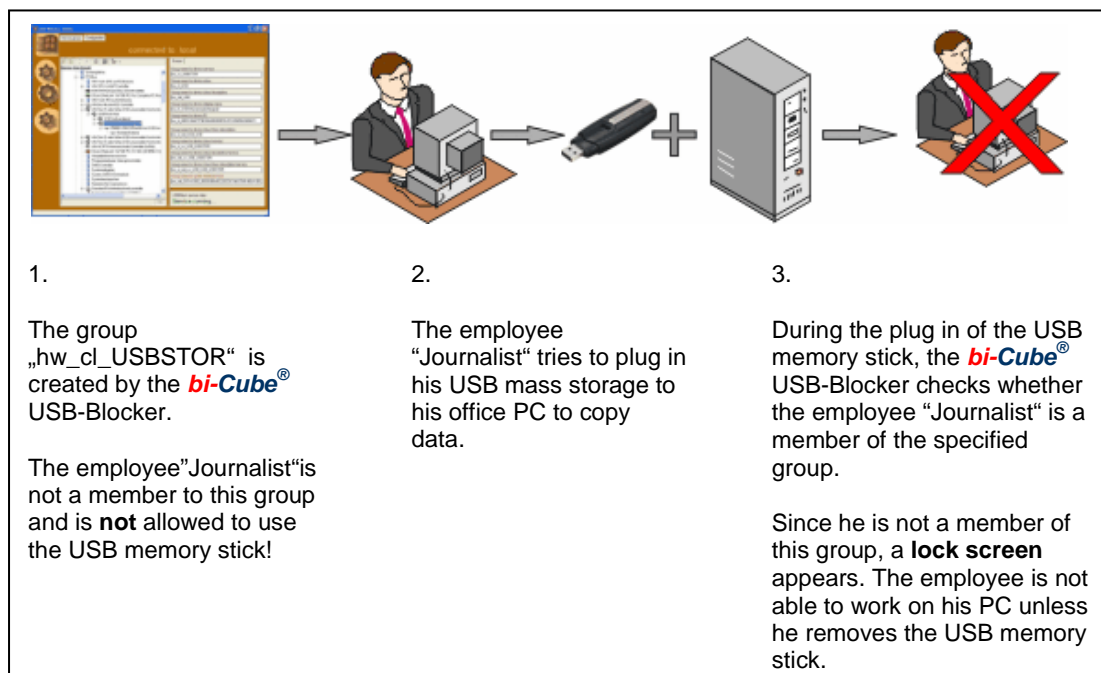
In case of locking or authorization for the storage media to be used, it is differentiated between device classes, service affiliation, device ID and additional properties. The **bi-Cube[®]** USB-Blocker analyses the different properties of the device. To ensure the unique identification of devices, these properties can be combined.

The **bi-Cube[®]** USB-Blocker recognises the device properties and checks if there is a corresponding user group available to this exact device type, determined by Windows and whether the logged on user is a member of this group. (These groups may exist in ADS or NDS.)

If the user is not a member of this group then the ejection mechanism of Windows is

activated and a message appears to inform the user about this process. During the ejection, the PC is locked so that the user is not able to influence this process in any way.

Besides the deactivation of internal devices and CD-Rom as well as disk drives, it is also possible to restrict the write access to the data medium.



4 Active Directory and Novell Directory Service

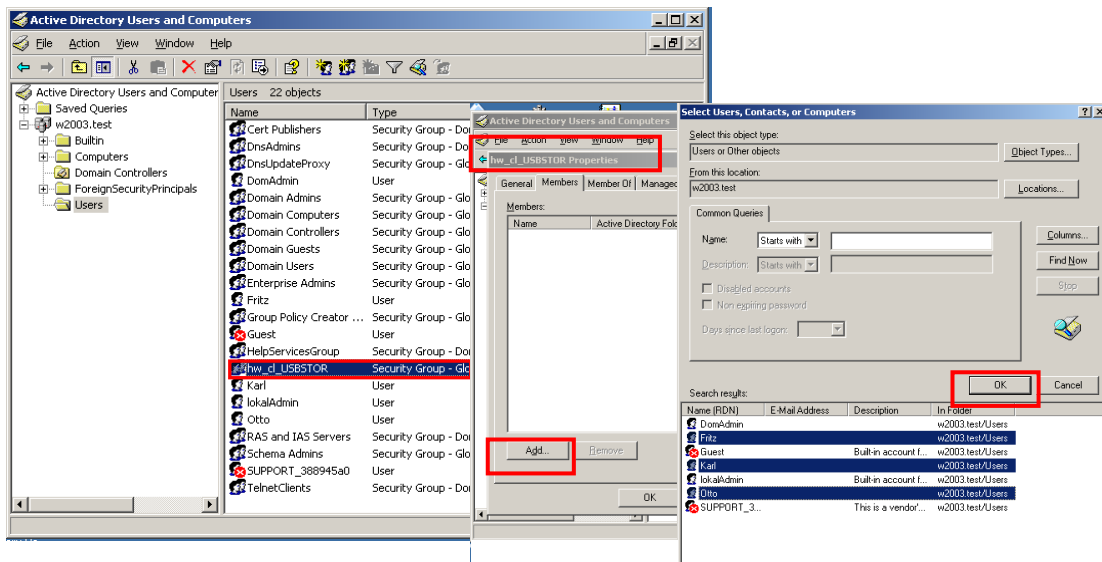
bi-Cube[®] USB-Blocker and ADS

By using the **bi-Cube[®]** USB-Blocker in networks with an Active Directory, local groups and ADS groups are analyzed.

Once the user logs on to his workstation, all groups which are relevant to the **bi-Cube[®]** USB-Blocker and group memberships in this ADS are queried and cached locally. This temporary storage serves to maintain the blocking function in case of none existing domain connection.

bi-Cube[®] USB-Blocker and NDS

By the connection of the **bi-Cube[®]** USB-Blocker to the NDS, a broad support of existing network infrastructures is possible. The configuration in the NDS is executed just as in the ADS via user groups which also enables a support of existing organizational structures in the NDS. The NDS function can be activated as an additional option.



Picture 2: Adding the user "Fritz", "Karl" and "Otto" to the group hw_cl_USBSTOR in the Active Directory. Since these users are now members of this group, the USB port access is authorized to them.

5 Analysis and Configuration Tool

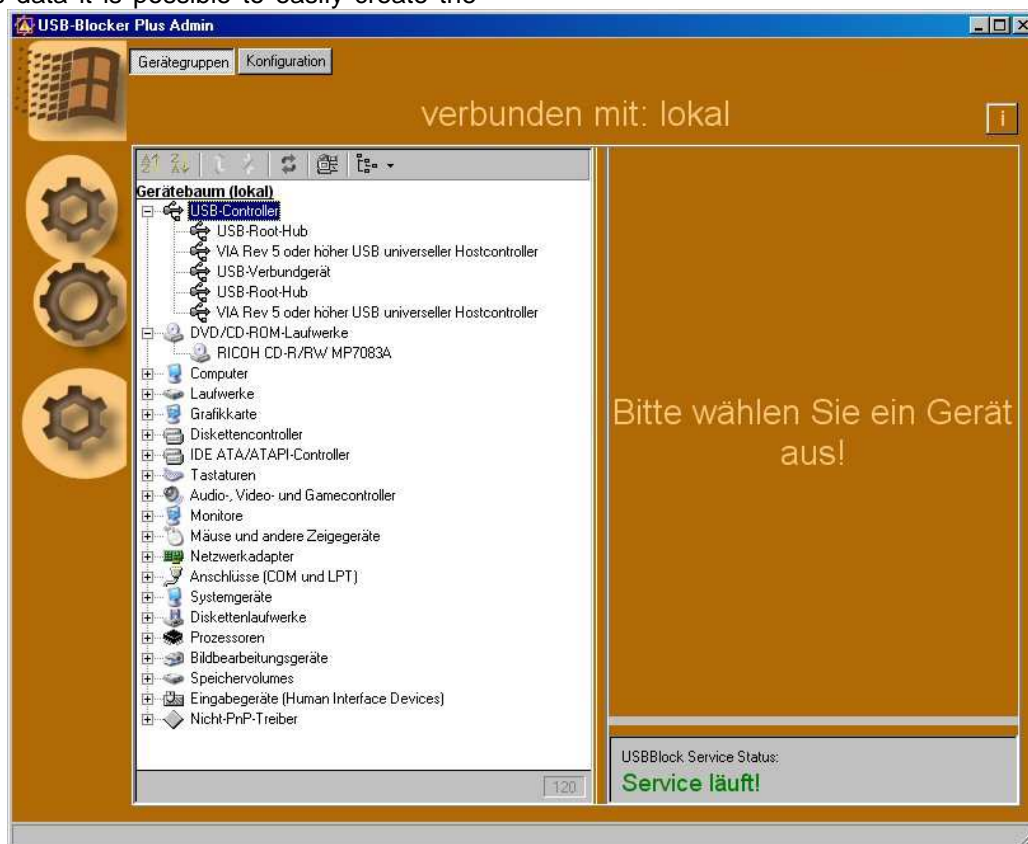
bi-Cube[®] USB-Block Admin

To implement this security function, it is required to analyze device properties and their context.

For analysis intentions, iSM has developed the **bi-Cube[®] USB-Blocker Admin** interface, which provides the required data to the administrator. By this data it is possible to easily create the

required groups on the local PC in the ADS or NDS.

In addition, this admin tool provides the option to comfortably perform each program setting via only one interface. This is an improvement and eases the job of the administrator, compared with previous time consuming configurations by different settings files.



6 Integrated in **bi-Cube[®]** IPM

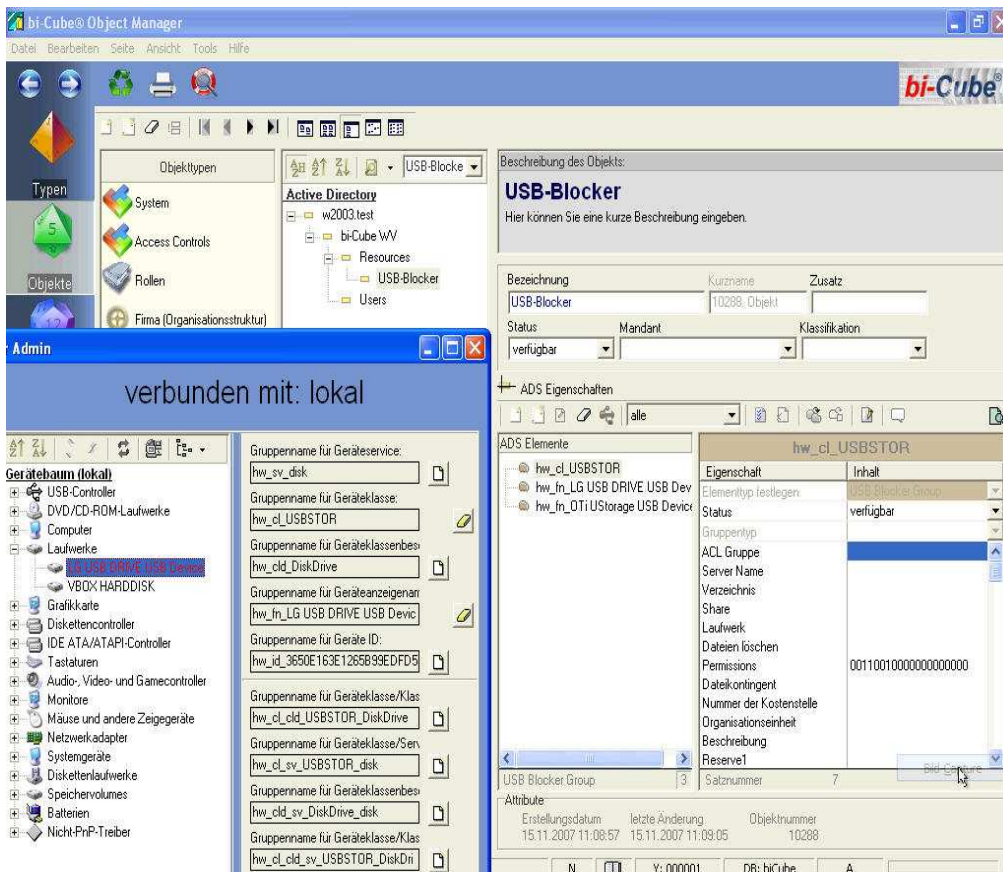
As integrated component in the developed solution of iSM's **bi-Cube[®]** IPM, it is also possible with the **bi-Cube[®]** USB-Blocker, to process an automatically and rule based allocation of authorizations, for external and internal hardware by roles.

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

The results represent a high security level and provide another reduction of administrative efforts.

The roles are centrally defined and locally assigned to the user, according to his competence or job position.

The employee automatically becomes member of a group in the Active Directory or Novell Directory and receives all for him required authorizations.



7 Key Benefits

- With the protection by the **bi-Cube[®]** USB-Blocker there is no connection available which enables the use of hardware components that are not released.
- The **bi-Cube[®]** USB-Blocker controls every change in the Device Manager. The outcome of this is the sustainability, because even not yet known devices can be ejected or deactivated in the future.
- By the control of permitted storage media the job of the IT management, to secure the networks in a company is greatly reduced.
- The **bi-Cube[®]** USB-Blocker is a security tool which protects next to the USB port, also fire wire interfaces or PCMCIA ports against unauthorized access.
- Depending on the logged on user, the different ports for the corresponding devices are either released, or locked. (Selection).
- By restricting the write access, the user may obtain read authorizations to e.g. USB memory sticks.
- The **bi-Cube[®]** USB-Blocker provides a broad support of existing network infrastructures because of the connection to the ADS and the NDS.
- Due to wildcard characters in both operating systems, it is possible to release different devices of one and the same developer by only one group. To express the wildcards “asterisk” or “question mark”, character combinations can be defined at the **bi-Cube[®]** USB-Blocker.
- By integrating the **bi-Cube[®]** USB-Blocker into the Identity & Provisioning Management of iSM's **bi-Cube[®]** IPM, the admins efforts are reduced and the functionalities in the area of authorization assignments, analysis and log functions are extended.

8 System Requirements (Without **bi-Cube[®]** Integration)

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

- Windows 7 (64bit) *
- Windows 7 (32bit)
- Windows VISTA (64bit)*
- Windows VISTA (32bit)
- Windows XP Professional/Home*1
- Windows 2008 Server
- Windows 2003
- Windows 2000 Professional
- Windows 2000 Server

* Supports basic functions such as locking or blocking of devices. At this time, without the support of the write-protect function.

To manage groups, the following systems are used:

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

Generally: Free memory space of 20 MB is required for the installation.

Note: Windows NT is not supported!

The **bi-Cube[®] USB-Blocker cannot not be installed on a domain controller!**

Installation type:

Demo version: Setup with optional language (German or English).

License version: Individual setup for every customer.
Creating MSI and MST packets for network distribution.