

Produktinformation

bi-Cube[®] USB – Blocker

Technologien Lösungen Trends Erfahrung

Inhalt

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

Firmeninterne Datensicherheitsrichtlinien werden zum Ärger vieler Administratoren durch die Mitarbeiter ignoriert bzw. sträflich vernachlässigt. So werden zum Beispiel über benutzerfreundliche USB-Sticks, CD-ROM, DVD, Diskette oder externe Festplatten häufig Daten ausgetauscht, ohne diese Geräte zuvor auf sensitive Datenbestände zu prüfen. Dadurch dringen immer wieder Viren trotz Firewall in Unternehmensnetze ein.

Eine weitere große Gefahr ist der Datendiebstahl über Speichermedien. Mitarbeiter beeinträchtigen unabsichtlich oder mutwillig durch Nutzung verschiedenster Massenspeichermedien die Sicherheit von Firmennetzwerken.

Durch den **bi-Cube[®] USB-Blocker** werden sämtliche Geräte des Gerätemanagers u.a. der Gebrauch von externen (USB-Stick) und eingebauten Speichermedien (CD-ROM- und Diskettenlaufwerke) an allen Clients im Unternehmen reglementiert.

Die Vorteile des **bi-Cube[®] USB-Blockers** sind:

- Erleichterung der Arbeit im IT-Risk-Management von Unternehmen
- Absicherung sämtlicher Schnittstellen (USB-Port, PCMCIA, Firewire)
- Zukunftsfähigkeit durch Aufbau des **bi-Cube[®] USB-Blocker** auf den Gerätemanager und der Reglementierung sämtlicher aufgeführter Geräte
- Kontrolle externer und interner Speichermedien
- Zugriffsteuerung durch Gruppenzugehörigkeit
- Unterscheidung einzelner Geräte oder ganzer Gerätegruppen möglich
- ADS und NDS Funktion

Die wirtschaftlichen Effekte sind:

- Massenspeichermedien stellen kein Risiko mehr da
- Verhinderung von Datendiebstahl und Schutz des Firmennetzwerkes
- geringer Kosten-, Integrations- und Installationsaufwand (keine zusätzlichen Server nötig)

Der **bi-Cube[®] USB-Blocker** sperrt nicht den gesamten Anschluss. Die Administratoren sind in der Lage, verschiedenste Hardwarekomponenten, wie Drucker oder Scanner für die Mitarbeiter weiter verfügbar zu stellen. Dabei kann zielgerichtet der Zugriff einzelner Benutzer gewährt oder verweigert werden.

2 Ausgangssituation

Durch die Anwendung von Speichergeräten entstehen mehrere Risiken:

- die unberechtigte Nutzung von Software (Lizenzverstöße)
- der unberechtigte Zugang zu Daten (Datenmanipulation)
- die unberechtigte Nutzung und Weitergabe von firmeninternen Daten (Datenschutz und Firmen-geheimnisse)
- der „Import“ von Viren.

Diese Risiken steigern den Druck auf das IT-Management die innere Sicherheit der Firmennetzwerke zu erhöhen.

Datendiebstahl oder Virenimport mit Hilfe von Speichermedien muss verhindert, jedoch die Arbeitsabläufe und Funktionen aller

Geschäftsprozesse nicht negativ beeinflusst werden.

Im ersten Schritt zur Sicherung der Firmennetzwerke kann durch den **bi-Cube[®]** USB-Blocker die Nutzung sämtlicher Speichermedien verboten werden. In der Regel ist es aber nicht möglich, den USB-Port gänzlich abzuschalten, da diverse (erlaubte) externe Geräte wie Scanner oder Drucker weiterhin verfügbar sein müssen.

Daher kann im zweiten Schritt dem User selektiv die Nutzung ausgewählter Geräte wieder erlaubt werden.

Durch den **bi-Cube[®]** USB-Blocker erfolgt der Zugriffsschutz über die Konfiguration des Speichermediums mit Hilfe allgemeiner Zugriffsschutzmechanismen im Active Directory oder Novell Directory.

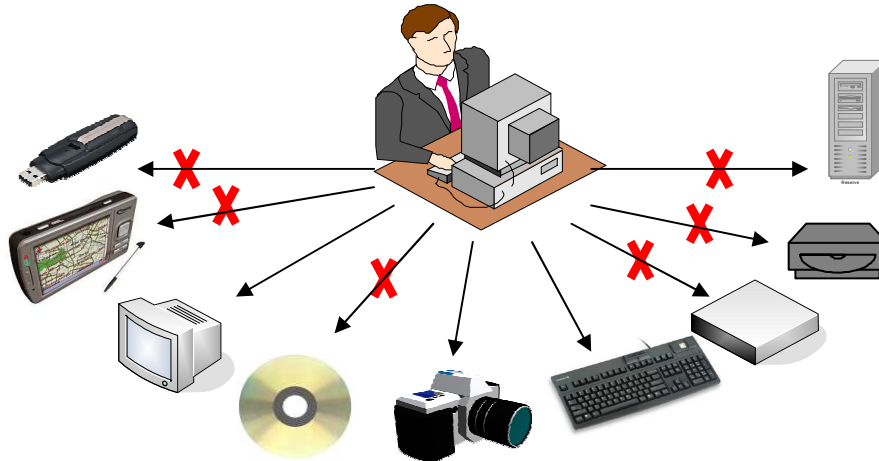


Abb. 1 Der Mitarbeiter „Journalist“ darf die Geräte Tastatur, Bildschirm und Kamera an seine lokale Arbeitsstation anschließen.

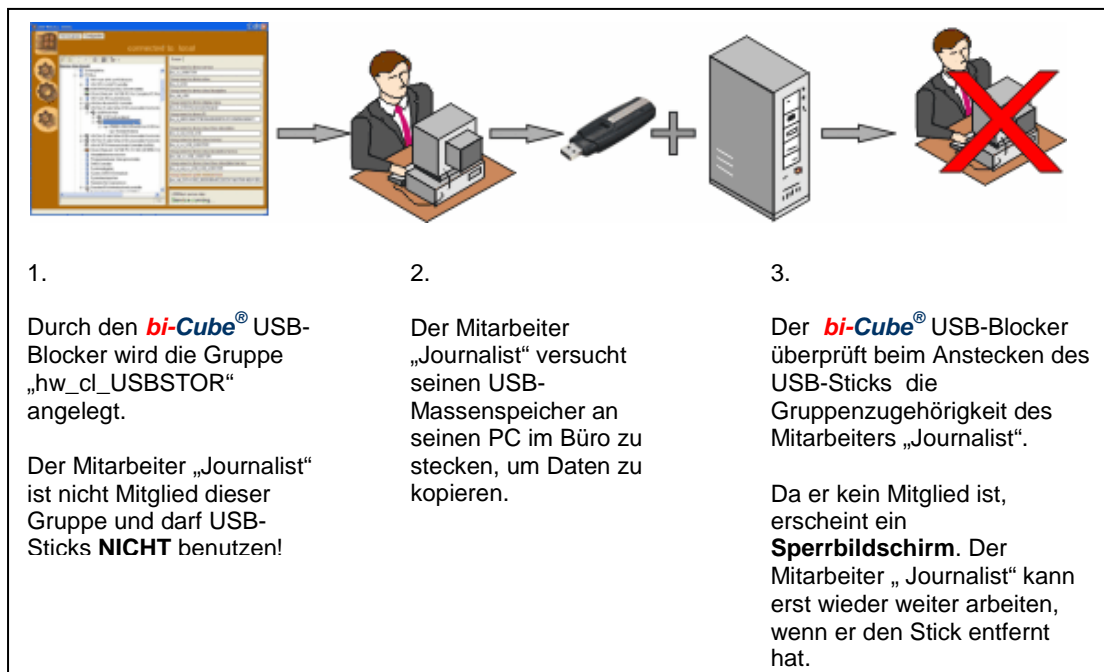
3 Funktionalität

Bei Sperrung bzw. Genehmigung der zu nutzenden Speichergeräte erfolgt eine Unterscheidung nach Geräteklassen, Servicezugehörigkeit, Geräte ID und weiteren Eigenschaften. Der **bi-Cube[®]** USB-Blocker wertet die verschiedenen Eigenschaften des zu nutzenden Gerätes aus. Um eine eindeutige Identifikation von Geräten zu gewährleisten, können zusätzlich diese Eigenschaften kombiniert werden.

Der **bi-Cube[®]** USB-Blocker erkennt beim Anstecken diese Geräte-Eigenschaften und prüft, ob es genau zu dem von Windows ermittelten Gerätetyp eine entsprechende Benutzergruppe gibt und der angemeldete User Mitglied einer dieser Gruppe ist. (Diese Gruppen können lokal sowie im ADS oder NDS vorhanden sein.)

Falls dieses nicht der Fall ist, wird der Auswurf-Mechanismus von Windows aktiviert und ein Fenster informiert über diesen Prozess. Während dieses Auswurfprozesses wird der PC gesperrt, damit der User in diesem Zeitraum keine Möglichkeit hat, in irgendeiner Form auf diesen Prozess Einfluss zu nehmen.

Neben der Deaktivierung interner Geräte wie CD-ROM und Diskettenlaufwerken, ist es weiterhin möglich den schreibenden Zugriff auf einen Datenträger einzuschränken.



4 Active und Novell Directory Service

bi-Cube[®] USB-Blocker im ADS

Bei Verwendung des **bi-Cube[®]** USB-Blocker in Netzwerken mit einem Active Directory werden lokale und ADS Gruppen ausgewertet. Meldet sich ein User am PC an, werden alle für den **bi-Cube[®]** USB-Blocker relevanten Gruppen und die Usermitgliedschaften in diesen im ADS abgefragt und lokal zwischengespeichert. Diese Zwischenspeicherung dient zur Aufrechterhaltung der Blockierfunktion bei nicht vorhandener Domänenverbindung.

bi-Cube[®] USB-Blocker im NDS

Durch die Anbindung des **bi-Cube[®]** USB-Blocker an das NDS ergibt sich eine breite Unterstützung vorhandener Netzwerk-Infrastrukturen. Die Konfiguration im NDS erfolgt in gleicher Weise wie im ADS über Benutzergruppen, die auch eine Unterstützung vorhandener Organisationsstrukturen im NDS ermöglicht. Die NDS Funktionalität ist als Zusatzoption aktivierbar.

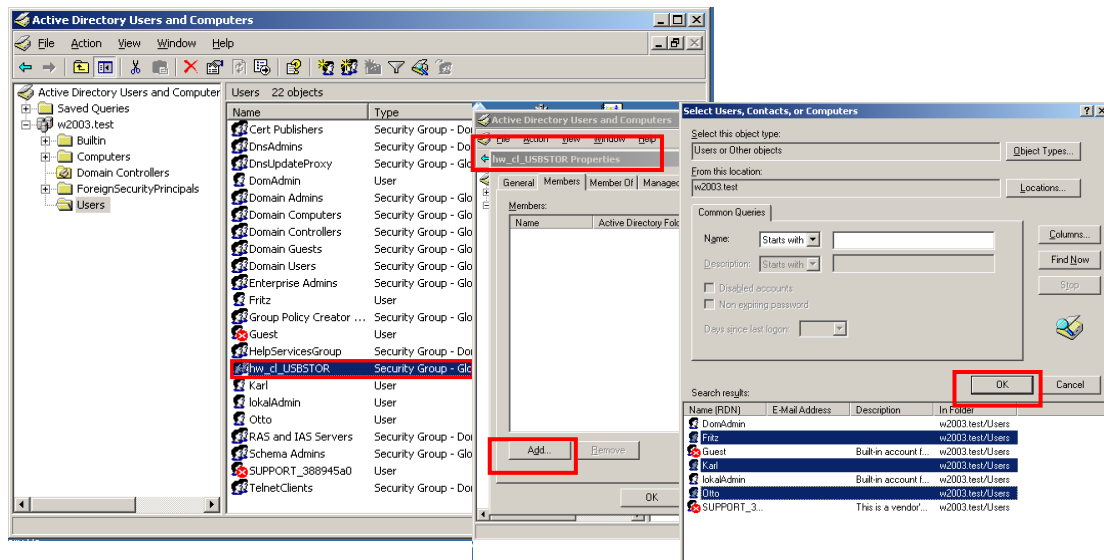


Abb. 2 Hinzufügen der User „Fritz“, „Karl“ und „Otto“ zu der Gruppe hw_cl_USBSTOR im Active Directory. Für diese User ist der USB-Port freigegeben.

5 Analyse- und Konfigurationswerkzeug

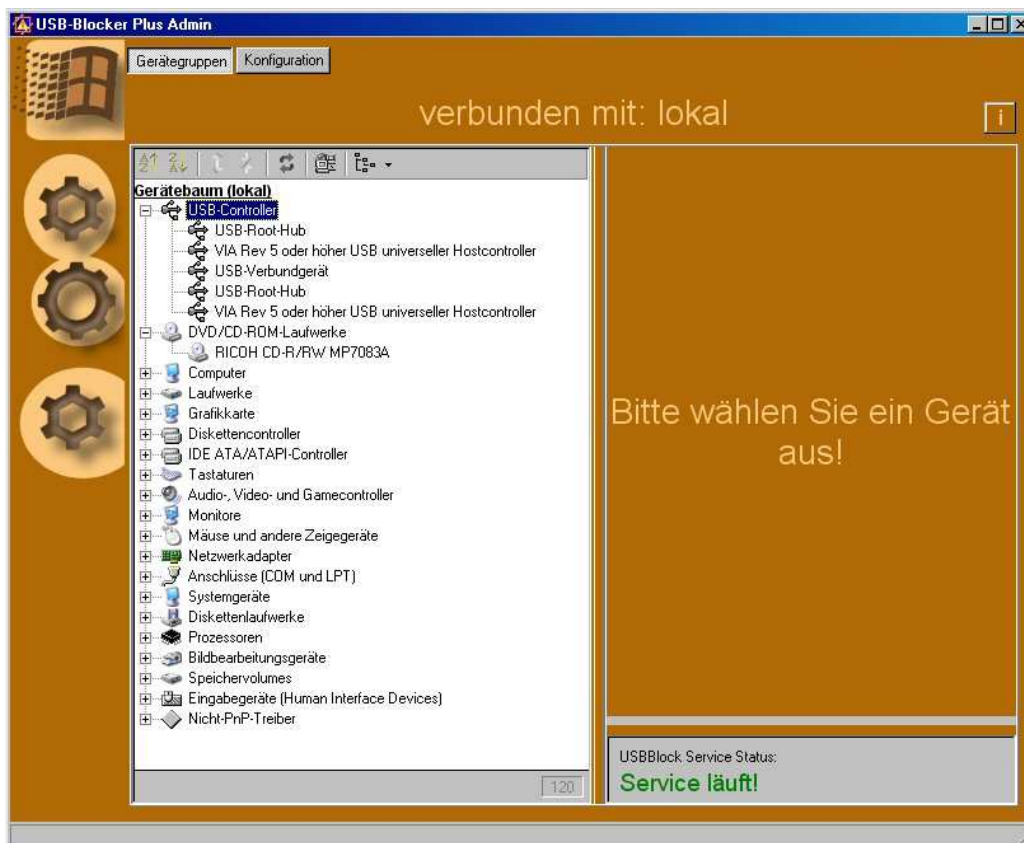
bi-Cube[®] USB-Block Admin

Um diese Sicherheits-Funktionen realisieren zu können, ist es erforderlich, die Geräte-Eigenschaften und deren Kontext auszuwerten.

Für Analyse Zwecke wurde deshalb vom iSM die **bi-Cube[®] USB-Blocker Admin** Oberfläche entwickelt, welche dem Administrator die dazu erforderlichen Daten zur Verfügung stellt. Mit diesen Daten ist es dann problemlos möglich,

die notwendigen Gruppen auf den lokalen PC's, im ADS oder NDS zu erstellen.

Weiterhin bietet das Administrationstool die Möglichkeit, die einzelnen Programmeinstellungen bequem über eine einzige Oberfläche zu tätigen. Dies stellt vor allem im Hinblick auf die Arbeit des Administrators eine Verbesserung gegenüber den Konfigurationen mit Hilfe von Einstellungsdateien dar und macht die Arbeit deutlich einfacher und komfortabler.



6 Integriert in **bi-Cube[®]** IPM

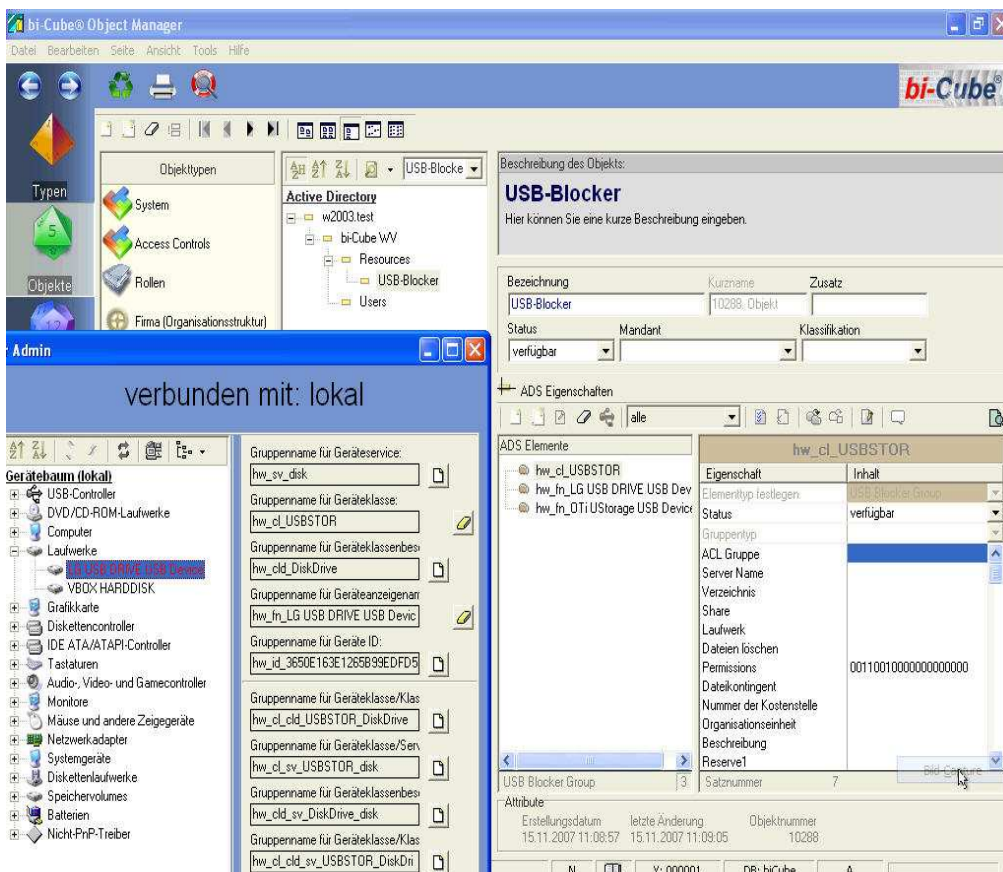
Als integrierte Komponente in der vom iSM entwickelten Lösung **bi-Cube[®]** IPM besteht zusätzlich die Möglichkeit eine automatische und regelbasierte Zuweisung von Berechtigungen für externe und interne Geräte über Rollen mit dem **bi-Cube[®]** USB-Blocker durchzuführen.

Das ausgereifte Rollenmanagement ermöglicht somit eine klare und strukturierte Zuordnung von Berechtigungsprofilen und ordnet sich optimal in die Aufbau und Prozessorganisation eines Unternehmens ein!

Die Ergebnisse sind ein hohes Security Niveau und eine weitere Senkung des Administrationsaufwands.

Die Rollen werden zentral definiert und dezentral der Kompetenz bzw. der Tätigkeit des Mitarbeiters zugeordnet.

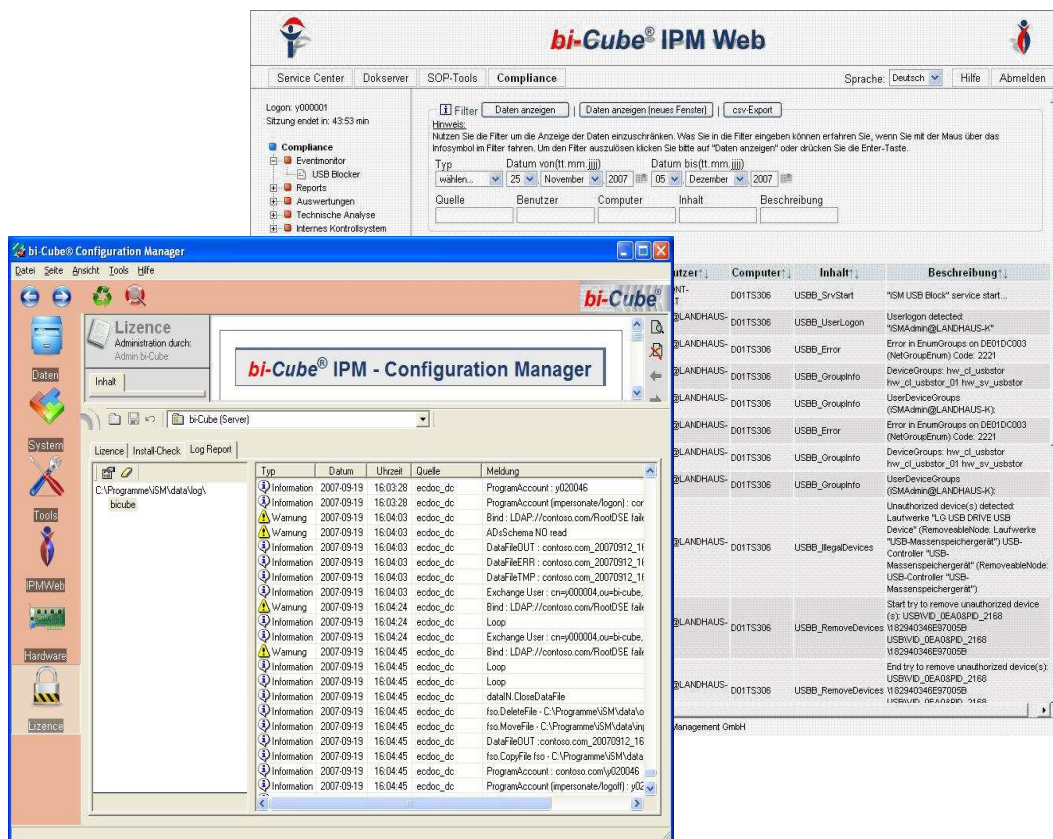
Der Mitarbeiter wird automatisch Mitglied in einer Gruppe im Active Directory oder Novell Directory und erhält sämtliche für ihn wichtigen Berechtigungen.



Ein weiterer Vorteil ist die umfangreiche **bi-Cube[®]** - basierende Auswertungs- und Logfunktion im neuen integrierten **bi-Cube[®]** USB-Blocker.

Somit stehen dem Administrator durch die Anbindung des **bi-Cube[®]** USB-Blocker an das Identity & Provisioning Management **bi-Cube[®]** viele neue Funktionalitäten zur Verfügung.

Mit Hilfe eines LogViewer werden alle lokalen Log-Dateien analysiert. Die **bi-Cube[®]** USB-Blocker-Events können komfortabel über eine Weboberfläche abgerufen und analysiert werden. Weiterhin besteht die Möglichkeit, die Reports der Weboberfläche in das bekannte csv-Format zu exportieren oder per automatisch generierter E-Mail zu versenden.



bi-Cube[®] IPM Web

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

Logon: y000001 Sitzung endet in: 43:53 min

Filter: Filter

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

Typ: wählen... Datum von (tt.mm.jjjj): 25 November 2007 Datum bis (tt.mm.jjjj): 05 Dezember 2007

Quelle	Benutzer	Computer	Inhalt	Beschreibung
BLANDHAUS		D01TS306	USB_SrvStart	"ISM USB Block" service start...
BLANDHAUS		D01TS306	USB_UserLogin	Userlogin detected "SMAAdmin@BLANDHAUS-K"
BLANDHAUS		D01TS306	USB_Error	Error in EnumGroups on DE01DC003 (NetGroupEnum) Code: 2221
BLANDHAUS		D01TS306	USB_GroupInfo	DeviceGroups: hrv_cl_usbstor hrv_cl_usbstor_01 hrv_sv_usbstor
BLANDHAUS		D01TS306	USB_GroupInfo	UserDeviceGroups (SMAAdmin@BLANDHAUS-K):
BLANDHAUS		D01TS306	USB_Error	Error in EnumGroups on DE01DC003 (NetGroupEnum) Code: 2221
BLANDHAUS		D01TS306	USB_GroupInfo	DeviceGroups: hrv_cl_usbstor hrv_cl_usbstor_01 hrv_sv_usbstor
BLANDHAUS		D01TS306	USB_GroupInfo	UserDeviceGroups (SMAAdmin@BLANDHAUS-K):
BLANDHAUS		D01TS306	USB_IllegalDevices	Unauthorized device(s) detected: Laufwerke "LG USB DRIVE USB Device" (RemoveableNode: Laufwerke "USB-Massenspeichergerät") USB-Controller "USB-Massenspeichergerät" (RemoveableNode: USB-Controller "USB-Massenspeichergerät")
BLANDHAUS		D01TS306	USB_RemoveDevices	Start try to remove unauthorized device(s): USB\VID_DEA0&PID_2168 1182940346&F700B
BLANDHAUS		D01TS306	USB_RemoveDevices	USB\VID_DEA0&PID_2168 1182940346&F700B
BLANDHAUS		D01TS306	USB_RemoveDevices	End try to remove unauthorized device(s): USB\VID_DEA0&PID_2168 1182940346&F700B

Management GmbH

bi-Cube[®] IPM - Configuration Manager

Lizence Administration durch: Admin bi-Cube

bi-Cube (Server)

Lizence | InstallCheck | Log Report

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/login) : cor
Warnung	2007-09-19	16:04:03	ecdoc_dc	Bind : LDAP://contoso.com/RootDSE fail
Warnung	2007-09-19	16:04:03	ecdoc_dc	AD+Schema NO read
Information	2007-09-19	16:04:03	ecdoc_dc	DataFileOUT : contoso.com_20070912_11
Information	2007-09-19	16:04:03	ecdoc_dc	DataFileERR : contoso.com_20070912_11
Information	2007-09-19	16:04:03	ecdoc_dc	DataFileTMP : contoso.com_20070912_11
Information	2007-09-19	16:04:03	ecdoc_dc	Exchange User : cny=000004.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 : cny=000004.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	fsso.DeleteFile : C:\Programme\ISM\data\o
Information	2007-09-19	16:04:45	ecdoc_dc	fsso.MoveFile : C:\Programme\ISM\data\inj
Information	2007-09-19	16:04:45	ecdoc_dc	DataFileOUT : contoso.com_20070912_16
Information	2007-09-19	16:04:45	ecdoc_dc	fsso.CopyFile fsso - 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/login) : y02

7 Key Benefits

- Durch die Absicherung mit dem **bi-Cube[®]** USB-Blocker steht kein Anschluss mehr zur Verfügung, über den nicht-freigegebene Hardwarekomponenten genutzt werden könnten.
- Der **bi-Cube[®]** USB-Blocker überwacht jede Veränderung im Gerätemanager. Daraus resultiert eine Zukunftsfähigkeit, so dass auch Geräte, die derzeit noch nicht bekannt sind, ausgeworfen oder deaktiviert werden können.
- Dem IT-Management in Unternehmen wird durch die Übersicht der erlaubten Speichermedien die Arbeit bei der Sicherung von Netzwerken erleichtert.
- Der **bi-Cube[®]** USB-Blocker ist ein Sicherheitstool, das neben dem USB-Port z.B. auch Firewire Schnittstellen oder den PCMCIA Port vor unbefugter Anwendung schützt.
- Je nach angemeldetem User wird die Nutzung der verschiedenen Ports für entsprechende Geräte freigegeben oder gesperrt (Selektion).
- Durch die Einschränkung des schreibenden Zugriffs erhalten die User Leserechte auf z.B. USB-Sticks
- Der **bi-Cube[®]** USB-Blocker bietet durch die Anbindung an das ADS und NDS eine breite Unterstützung vorhandener Netzwerkinfrastrukturen.
- Durch Wildcards ist es in beiden Betriebssystemen möglich, verschiedene Geräte desselben Herstellers mit nur einer Gruppe freizugeben. Um die Wildcards „Stern“ und „Fragezeichen“ auszudrücken, können beim **bi-Cube[®]** USB-Blocker Zeichenkombinationen definiert werden.
- Integriert in das Identity & Provisioning Management des iSM **bi-Cube[®] IPM** wird der Administrationsaufwand weiter gesenkt und zusätzlich erhöhen sich die Funktionalitäten im Bereich Berechtigungsvergabe und Auswertungs- und Logfunktion.

8 Systemvoraussetzungen (ohne **bi-Cube[®]** Integration)

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

- 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

* unterstützt Basisfunktionen wie das Sperren bzw. blockieren von Geräten, vorerst ohne Unterstützung der Schreibschutzfunktion

Für die Verwaltung der Gruppen können folgende Systeme herangezogen werden:

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

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

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

Installationsform:

Demoversion: Setup mit Auswahl für deutsche oder englische Sprache.

Lizenzversion: Individuelles Setup für jeden Kunden. Erstellung von MSI und MST Paketen zur Verteilung im Netzwerk.