USBSecure Professional 4.4

Schnittstellen-Sicherheit für Windows 7, Windows 8 und Windows 10

Installations- und Konfigurationsanleitung

USBSecure Professional 4.4

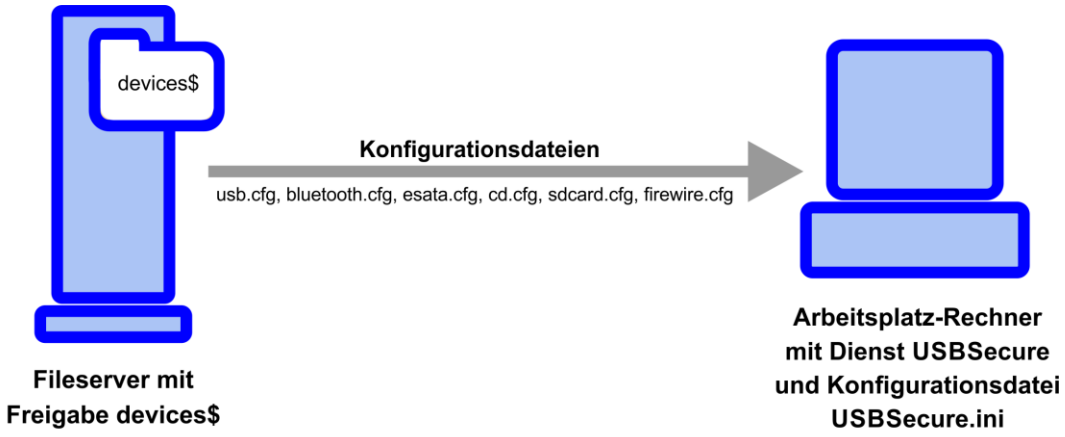
Installations- und Konfigurationsanleitung

Inhalt

Funktionsweise

USBSecure Professional ist eine Sicherheitssoftware zur Absicherung der USB-Schnittstelle. Sie können mit USBSecure Professional pro Benutzer oder pro Computer konfigurieren, auf welche USB-Geräte der Benutzer Zugriff hat. Zusätzlich lassen sich mit USBSecure Professional auch Bluetooth-Verbindungen, CD/DVD-Laufwerke, Disketten-Laufwerke, eSATA-Geräte, die Firewire-Schnittstelle und SD-Card-Reader benutzerbezogen ein- bzw. ausschalten.

USBSecure Professional läuft als Dienst unter Windows 7, Windows 8 und Windows 10 (32 oder 64 Bit). In Konfigurationsdateien wird der Zugriff auf USB-Geräte, Disketten- und CD/DVD-Laufwerke, eSATA-Geräte sowie die FireWire-Schnittstelle und SD-Card-Reader geregelt. Sobald ein Benutzer sich anmeldet, werden die Geräte bzw. Schnittstellen anhand der (vom Server kopierten) lokalen Konfigurationsdateien ein- bzw. ausgeschaltet. Als USBSecure-Server kann ein bereits vorhandener Fileserver oder ein beliebiger Windows-Server mit verwendet werden, lediglich eine Freigabe wird benötigt.
Zusätzlich zum USBSecure-Dienst wird bei der Installation ein geplanter Task (Aufgabe) installiert, der beim Hochfahren des Computers den Prozess USBSecureControl.exe startet. Dieser Prozess überwacht den Dienst USBSecure und startet ihn neu, falls er unerwartet beendet wurde.



Installation

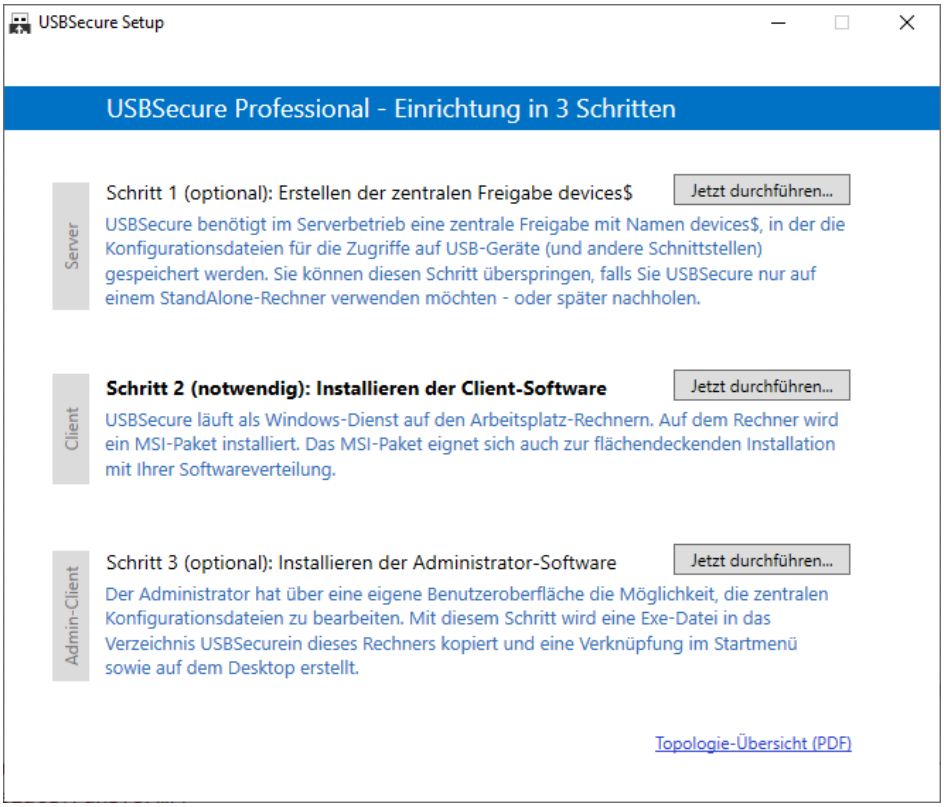
Systemvoraussetzungen

Clients: Der eigentliche USBSecure-Dienst (Sperren / Freigeben von Geräten und Schnittstellen) ist ohne jegliche .NET-Framework-Software lauffähig. Für die einwandfreie Interaktion mit dem Benutzer ist .NET-Framework 3.5 oder höher notwendig. Zur Information: Ab Windows 7 ist .NET-Framework 3.5 standardmäßig installiert.

Server: Da der Server lediglich aus einer Windows-Freigabe (Share) besteht, auf die alle Benutzer Leserechte besitzen, kann hier jeder Windows-Server (oder Client) ohne Einschränkung genutzt werden. Auch der Einsatz eines Filers oder NAS-Gerätes ist möglich.

Installation der Workstation (Client)

Sie können die Client-Installation manuell über die Datei Setup.exe ausführen und dann Schritt 2 wählen. Dadurch wird die Datei USBSecure.msi ausgeführt. Alternativ lässt sich das MSI-Paket auch über Ihre Softwareverteilung oder über Gruppenrichtlinien auf die Clients verteilen.



1. Führen Sie die Datei USBSecure.msi (Schritt 2) mit Administrator-Rechten auf dem zu schützenden Rechner aus. Während der Installation werden der USBSecure-Zielpfad und der Name des USBSecure-Servers abgefragt. Den Namen des USBSecure-Servers können Sie auch nachträglich noch in der Datei USBSecure.ini eintragen oder ändern. Sie benötigen zur Installation einen gültigen Lizenzschlüssel. Bei der kostenlosen 5-PC-Version befindet sich der Lizenzschlüssel als Textdatei im Download.
2. Achtung: Bevor Sie den USBSecure-Dienst starten, beachten Sie bitte, dass es möglich sein kann, dass USBSecure Ihren Fingerabdruckscanner deaktiviert! Falls Sie sich über Fingerabdruck anmelden, sollten Sie sich über Ihr Kennwort bewusst sein.
3. Starten Sie den Dienst "USBSecure". Im USBSecure-Verzeichnis wird daraufhin die Logdatei ***USBSecure.log*** erzeugt.

Testen der Client-Installation

Sie können USBSecure Professional nun im reinen Clientbetrieb ohne Server testen. Durch die jetzt vorhandene Datei usb.cfg ist durch den Eintrag „service = hidusb“ lediglich der Betrieb von USB-Mäusen und Tastaturen für alle Benutzer sowie alle Geräte für den Benutzer Administrator erlaubt. Die Einträge „service = usbhub“ und „service = usbhub3“ sollten immer vorhanden sein.

Schließen Sie nun einen USB-Massenspeicher an den Rechner an, z.B. einen USB-Stick. Da laut usb.cfg USB-Massenspeicher nicht erlaubt sind (außer für Benutzer Administrator), wird der USB-Stick deaktiviert (s. Geräte-Manager und USBSecure.log).
Fügen Sie nun in der Datei usb.cfg im Bereich [AllUsers] den Eintrag „service = usbstor“ hinzu und

starten Sie den Dienst USBSecure neu. Der USB-Massenspeicher wird nun aktiviert und erscheint als Laufwerk im Windows Explorer.

Hinweis für Windows 7/8/10: Sie müssen Ihren Editor „Als Administrator ausführen“, um die Datei usb.cfg bearbeiten zu können – auch wenn Sie bereits als Administrator angemeldet sind.

Lesen Sie im Abschnitt „Konfiguration“, wie Sie den Zugriff auf einzelne Geräte erlauben und wie Sie die Konfiguration pro Benutzer einrichten.

Hinweis: Die Gruppe "Benutzer" darf im späteren Betrieb keine Schreibrechte auf die Dateien im USBSecure-Verzeichnis besitzen.

Silent Installation

Die Installation ohne Benutzereingriff können Sie folgendermaßen durchführen:

msiexec /i USBSecure.msi /qb USBSECURE_SERVERNAME=<Name des Servers> INSTALLDIR="C:\Program Files (x86)\USBSecure" LICENSEKEY=AAAAA-BBBBB-CCCCC-DDDDD-EEEEE

Geben Sie nach **LICENSEKEY=** Ihren Lizenzschlüssel an. Den Lizenzschlüssel für die kostenlose 5-PC-Version finden Sie als Textdatei im Download.

Weitere Werte, die bei der automatischen Installation gesetzt werden können:

INIOVERWRITE=<Zeit in Minuten>
Gibt an, nach wieviel Minuten die lokale Konfigurationsdatei USBSecure.ini von einer möglichen zentralen USBSecure.ini überschrieben wird. <Zeit in Minuten> gibt die Zeit in Minuten nach Start des USBSecure-Dienstes an. Dieser Wert wird in die USBSecure.ini übernommen. Beispiel: INIOVERWRITE=15

NOUSBSTORINFO=<yes|no|warn>
Bestimmt das Verhalten bei Einstecken eines verbotenen USB-Massenspeichers (s. USBSecure.ini) Dieser Wert wird in die USBSecure.ini übernommen. Beispiel: NOUSBSTORINFO=no

ADMINSCANTSTOP=<0|1>
Bestimmt, ob der USBSecure-Dienst von Administratoren gestoppt bzw. durchgestartet werden darf. ADMINSCANTSTOP=1 bedeutet, dass Administratoren den Dienst nicht stoppen und durchstarten können. Dieser Wert wird nicht in die USBSecure.ini übernommen. Beispiel: ADMINSCANTSTOP=0

NETWORKADMINSCANSTOP=<0|1>
Nur in Verbindung mit ADMINSCANTSTOP. Bestimmt, ob der USBSecure-Dienst von Administratoren über das Netzwerk gestoppt bzw. durchgestartet werden darf. Bitte beachten Sie, dass es sich hierbei um „CAN“ handelt, beim vorhergehenden Wert um „CAN’T“. NETWORKADMINSCANSTOP =1 bedeutet, dass Administratoren den Dienst über das Netzwerk stoppen und durchstarten können. Dieser Wert wird nicht in die USBSecure.ini übernommen. Beispiel: NETWORKADMINSCANSTOP =1

Die Deinstallation erfolgt mit: **msiexec /x USBSecure.msi /qb**

Installation des Servers

Erstellen Sie auf einem beliebigen Windows-Server (oder einer Workstation, die als Server dienen soll) eine Windows-Freigabe "devices$". Gewähren Sie der Gruppe "Jeder" (Everyone) Leserechte auf das Verzeichnis und auf die Freigabe. Kopieren Sie die Dateien ***floppy.cfg***, ***cd.cfg, firewire.cfg, esata.cfg, sdcard.cfg*** und ***usb.cfg*** in das Verzeichnis. Die Dateien finden Sie in der Workstation-Installation im USBSecure-Verzeichnis.

Hinweis: Der USBSecure-Server und der Client müssen sich innerhalb derselben Windows-Domäne befinden.

Hinweis: Sollte sich Ihre Freigabe devices$ nicht auf einem Windows-Server, sondern auf einem Storagesystem (Filer) befinden, kann es sein, dass der Zugriff auf die Freigabe nicht funktioniert. Besonders geclusterte Systeme verhalten sich teilweise nicht exakt wie Windows-Server. Verwenden Sie hier nicht den Clusternamen, sondern den tatsächlichen Namen eines Nodes.

Testen der Server-Installation

1. Ändern Sie nun in Ihrer Client-Installation in der Datei USBSecure.ini den Wert hinter „Server=“ auf den Computernamen Ihres USBSecure-Servers. Wenn der Computername Ihres USBSecure-Servers beispielsweise Fileserver1 lautet, ändern Sie die Zeile in Server=Fileserver1.
2. Ändern Sie in der in der zentralen usb.cfg (auf Ihrem USBSecure-Server) die vorher hinzugefügte Zeile **service=USBSTOR** nach **#service=USBSTOR** ab oder löschen Sie sie komplett. Das Raute-Zeichen dient als Kommentar-Zeichen, so dass die Zeile ignoriert wird.
3. Beenden Sie den USBSecure-Dienst auf Ihrem Client und starten Sie ihn neu. Beim Neustart des Dienstes werden die Konfigurationsdateien (usb.cfg, cd.cfg, floppy.cfg, firewire.cfg und esata.cfg) vom USBSecure-Server auf den Client kopiert. Vergewissern Sie sich, dass in Ihrer lokalen usb.cfg (auf Ihrem Client unter C:\Programme\USBSecure) der Eintrag **service=USBSTOR** wie in der zentralen usb.cfg entfernt oder auskommentiert ist.

Alle USB-Massenspeicher werden nun deaktiviert.

Wenn der Zugriff auf den Server nicht funktioniert

Wenn der Zugriff auf den Server nicht funktioniert (zentrale usb.cfg wird beim Starten des USBSecure-Dienstes nicht auf den lokalen Client kopiert), stellen Sie bitte folgendes sicher:

- Server und Client befinden sich in der selben Windows-Domäne.
- Auf die devices$-Freigabe besitzt die Gruppe **Jeder** (bei englischem Betriebssystem: **Everyone**) Lesezugriff.
- Auf das devices$-Verzeichnis hat die Gruppe **Jeder** NTFS-Leseberechtigungen.

Überprüfen Sie mit folgendem Befehl (aus einer Eingabeaufforderung), ob der Zugriff für den aktuell angemeldeten Benutzer funktioniert:

`copy \\Servername\devices$\usb.cfg`
(verwenden Sie statt „Servername“ den Namen Ihres USBSecure-Servers)

Wenn der Kopiervorgang funktioniert, muss als nächstes sicher gestellt werden, dass auch der USBSecure-Dienst in der Lage ist, den Kopiervorgang durchzuführen. Führen Sie dazu folgenden Test durch.

Für Windows XP

Starten Sie auf Ihrem Client eine Eingabeaufforderung als lokaler System Account. Öffnen Sie dazu eine Eingabeaufforderung und geben folgenden Befehl ein:

`at 10:36 /INTERACTIVE cmd.exe`

Statt 10:36 Uhr geben Sie hier die aktuelle Uhrzeit plus 2 Minuten an. Wenn es beispielsweise gerade 14:09 Uhr ist, geben Sie 14:11 an. Falls hier „Zugriff verweigert“ erscheint, melden Sie sich bitte als Administrator an. Um 14:11 Uhr wird sich dann eine Eingabeaufforderung öffnen, in der Sie den copy-Befehl eingeben:

`copy \\Servername\devices$\usb.cfg`
(verwenden Sie statt „Servername“ den Namen Ihres USBSecure-Servers)

Wenn sich die Datei auf diese Art kopieren lässt, ist auch der USBSecure-Dienst in der Lage, sie zu kopieren.

Für Windows Vista / Windows 7 / Windows 8 / Windows 10

Laden Sie die PS Tools von Microsoft Sysinternals (www.sysinternals.com) herunter und führen Sie auf Ihrem Client folgenden Befehl in einer Eingabeaufforderung („als Administrator ausgeführt“) aus: `psexec -i -s cmd.exe`

Geben Sie in der neu geöffneten Eingabeaufforderung den copy-Befehl ein:

`copy \\Servername\devices$\usb.cfg`
(verwenden Sie statt „Servername“ den Namen Ihres USBSecure-Servers)

Wenn sich die Datei auf diese Art kopieren lässt, ist auch der USBSecure-Dienst in der Lage, sie zu kopieren.

Falls der Kopiervorgang nicht funktioniert und sich Ihre devices$-Freigabe auf einem Storagesystem befindet, versuchen Sie zunächst, einen „echten“ Windows-Server als USBSecure-Server einzusetzen. Unter Umständen verhält sich das Storagesystem nicht exakt Windows konform.

Der Dienst USBSecure

Der Dienst „USBSecure“ lässt sich von Benutzern und Hauptbenutzern nicht stoppen. Administratoren haben das Recht, den Dienst zu stoppen und zu starten. Ausnahme: Während der Installation wurde Administratoren das Recht entzogen, den Dienst zu beenden.

Deinstallation

Die Deinstallation erfolgt über die Systemsteuerung / Programme und Funktionen.

Achtung: Bitte beachten Sie, dass USB-Geräte, die vom USBSecure-Dienst deaktiviert wurden, bei der Deinstallation der Software nicht wieder aktiviert werden. Geben Sie daher vor der Deinstallation alle USB-Geräte für den betreffenden Benutzer oder alle Benutzer frei mit

[AllUsers]
*

und starten Sie den USBSecure-Dienst neu oder aktivieren Sie die Geräte nachträglich über den Gerätemanager.

Upgrade von einer älteren Version

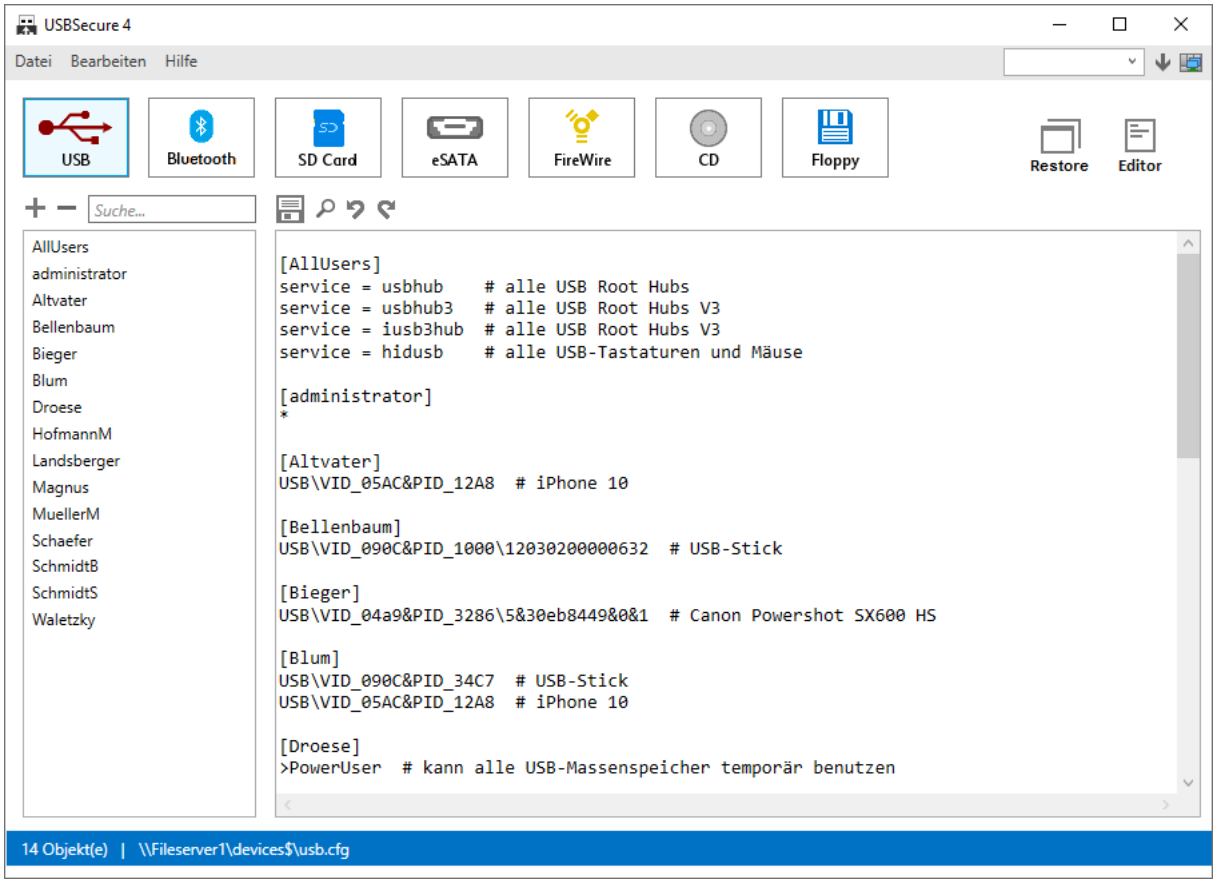
Das Upgrade von einer älteren USBSecure-Version besteht immer aus einer Deinstallation und Neuinstallation. Konfigurationseinstellungen bleiben bei einer Netzwerkinstallation erhalten, da sie zentral in der devices$-Freigabe gespeichert sind. Bei einer lokalen Installation (Standalone) sollten Sie vor der Deinstallation alle .cfg-Dateien wegsichern in später wieder ins Verzeichnis kopieren.

Wenn Sie eine Netzwerkinstallation von einer älteren Version auf Version 4.4 aktualisieren, ist folgendermaßen vorzugehen:

1. Kopieren der Datei bluetooth.cfg aus dem Verzeichnis „Server“ des Installationsmediums in Ihre vorhandene devices$-Freigabe.
2. Ersetzen der Administrationsoberfläche USBSecure-Admin.exe durch die neue Version aus dem Verzeichnis „Admin“ des Installationsmediums.
3. Neuinstallation der Client-Software USBSecure.msi aus dem Verzeichnis „Client“ des Installationsmediums.

Konfiguration

Ab USBSecure Professional 4.0 können die Whitelists (.cfg-Dateien) über eine grafische Administrationsoberfläche konfiguriert werden. Die Administrationsoberfläche setzt .NET-Framework 4.5 auf Ihrem Computer voraus. Eine direkte Konfiguration der Dateien per Editor ist weiterhin möglich.



Die Konfigurationsdateien

Die Konfigurationsdateien ***usb.cfg***, ***bluetooth.cfg***, ***cd.cfg, firewire.cfg, esata.cfg, sdcard.cfg*** und ***floppy.cfg*** dienen als Whitelists für erlaubte Geräte. Benutzer, die nicht in den Dateien aufgeführt sind, haben keinen Zugriff auf die Geräte. Eine Ausnahme bildet der [AllUsers]-Bereich in der usb.cfg und der der bluetooth.cfg bzw. der AllUsers-Eintrag in den Dateien floppy.cfg, cd.cfg, firewire.cfg, sdcard.cfg und esata.cfg. Die .cfg-Dateien werden in der zentralen Freigabe devices$ gepflegt und bei jedem Dienststart des Clients in das USBSecure-Verzeichnis kopiert. Der Zugriff des USBSecure-Dienstes erfolgt immer auf die lokal abgelegten Dateien.

Bei der Datei USBSecure.ini handelt es sich um eine statische Datei auf dem Rechner des Anwenders. Hier werden globale Einstellungen (Name des USBSecure-Servers, Loglevel usw.) vorgenommen.

Neu ab USBSecure Professional Version 3: Der Parameter **IniOverwrite**, um trotzdem eine zentrale Verwaltung der USBSecure.ini zu ermöglichen (s.u.).

floppy.cfg, cd.cfg, firewire.cfg, esata.cfg und sdcard.cfg

Benutzer, die Zugriff auf Disketten- und CD-Laufwerke, den FireWire-Port, eSATA-Geräte und SD-Cards haben sollen, werden in den Dateien ***floppy.cfg, cd.cfg, firewire.cfg, esata.cfg und sscard.cfg*** aufgelistet (ein Benutzer pro Zeile):

```
UserA
UserB
UserC
```

Sollen alle Benutzer Zugriff auf die jeweiligen Geräte bzw. Schnittstellen bekommen, wird in der entsprechenden Datei der Wert „AllUsers“ eingetragen:

```
AllUsers
```

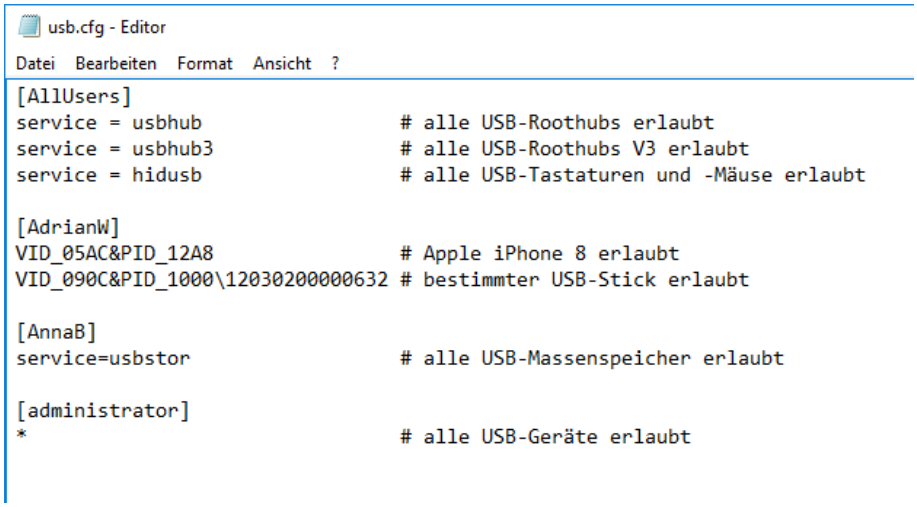
Im Gegensatz zu USB-Geräten lässt sich bei Diskettenlaufwerken, CD/DVD-Laufwerken, Firewire-Schnittstellen, eSATA-Schnittstellen und SD-Cards der Zugriff auf einzelne, bestimmte Geräte nicht konfigurieren. Sobald ein Benutzer in der entsprechenden .cfg-Datei eingetragen ist, ist der Zugriff auf alle Geräte des Typs erlaubt.

usb.cfg

In der Datei ***usb.cfg*** wird der Zugriff auf USB-Geräte geregelt. Dabei werden die Benutzernamen in eckigen Klammern angegeben. Nach dem Benutzernamen werden jeweils die erlaubten USB-Geräte aufgeführt. Datei usb.cfg enthält einen AllUsers-Bereich und einen Bereich pro Benutzer:

```
[AllUsers]
…

[BenutzerA]
…

[BenutzerB]
…

[BenutzerC]
…
```

Die Bezeichnungen der USB-Geräte stammen aus der Registry. Das Skript ***ShowExistingUsbDevices.vbs*** (als Administrator ausgeführt) erzeugt die Datei ***ExistingUsbDevices.txt***, in der alle auf dem Rechner installierten USB-Geräte in der gewünschten Notation aufgelistet sind. Damit können sie bequem in die ***usb.cfg*** übernommen werden.



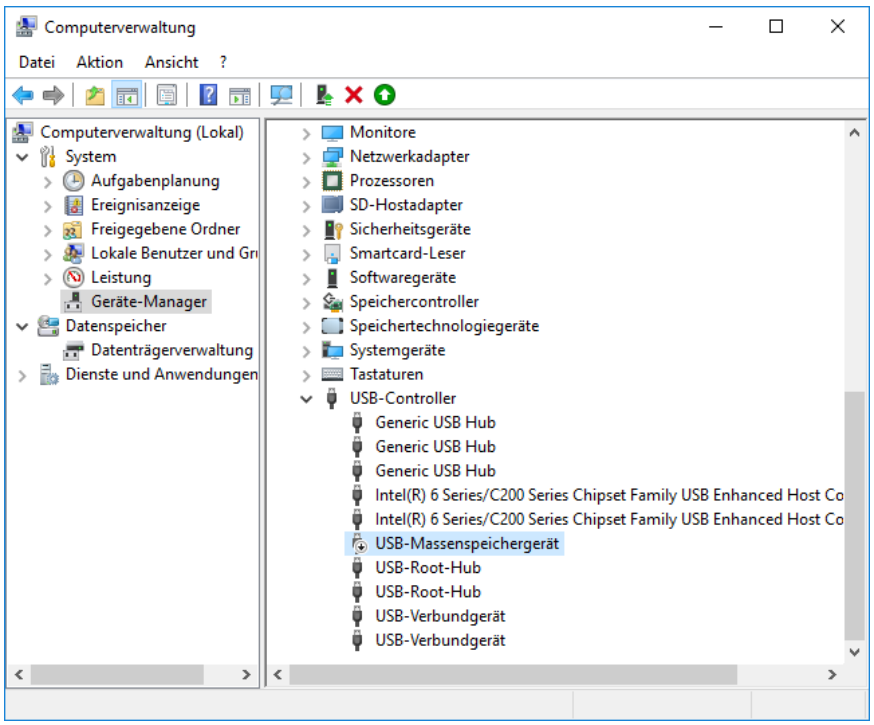
Sämtlicher Text hinter der Raute (#) dient als Kommentar zur besseren Lesbarkeit.

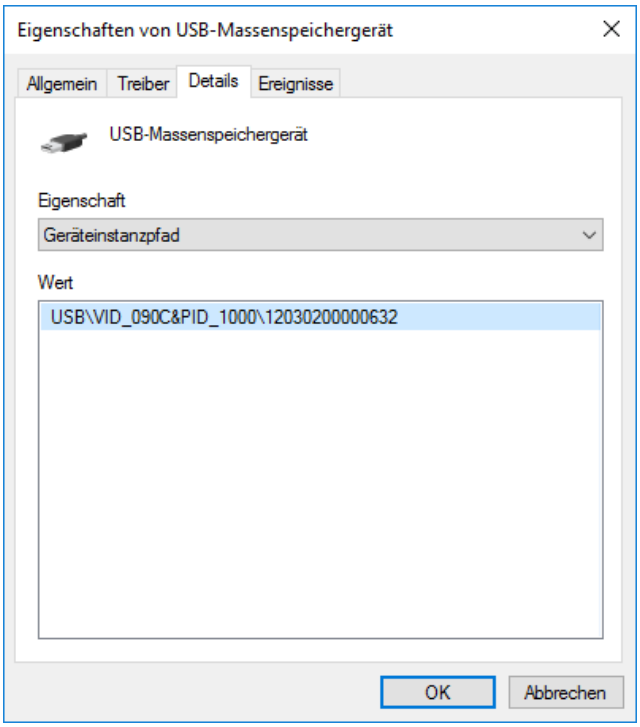
Privilegierte Benutzer mit Zugriff auf alle USB-Geräte erhalten einen Stern (*):

```
[UserA]
*
```

Im Bereich [AllUsers] werden Geräte aufgeführt, die für alle Benutzer freigegeben sind. Hier sollten zumindest immer die Zeilen „service = usbhub“ und „service = usbhub3“ aufgelistet sein sowie "ungefährliche" Geräte wie Mäuse, Tastaturen und Scanner.
Die Konfiguration eines Benutzer ergibt sich immer aus der **Summe der AllUsers-Konfiguration und der persönlichen Konfiguration**. Sind beispielsweise im AllUsers-Bereich alle USB-Roothubs und alle USB-Mäuse und –Tastaturen freigegeben und im persönlichen Bereich des Benutzers alle USB-Massenspeicher, dann sind für den Benutzer alle USB-Roothubs, alle USB-Mäuse und –Tastaturen und alle USB-Massenspeicher freigegeben.

Alternativ lässt sich die Vid/Pid-Kennung auch direkt über den Geräte-Manager in den Eigenschaften des USB-Gerätes herausfinden. Im folgenden Beispiel wird als Kennung **VID_090C&PID_1000\12030200000632** eingetragen, um genau diesen USB-Massenspeicher freizugeben.





Die Schreibweise USB\VID_090C&PID_1000\12030200000632 mit vorangestelltem USB\ ist ebenfalls erlaubt, so dass die ID direkt aus dem Gerätemanager über rechte Maustaste / Kopieren herauskopiert werden kann.

Sollen alle USB-Massenspeicher des gleichen Typs freigeschaltet werden, kann als ID der Wert VID_090C&PID_1000 verwendet werden (analog ist USB\VID_090C&PID_1000 ebenfalls erlaubt).

Wildcard Fragezeichen

Verwenden Sie das Fragezeichen „?“, um einen Platzhalter für ein Zeichen zu setzen:

VID_1234&PID_????

Damit ist es möglich, alle Geräte eines bestimmten Herstellers zu erlauben: Man gibt die VID (Vendor ID) an und lässt die PID (Product ID) variabel. Um beispielsweise alle Geräte des Herstellers Kyocera zu erlauben, könnten Sie folgenden Ausdruck verwenden: VID_0482&PID_????

Groß-/Kleinschreibung

Die Groß-/Kleinschreibung ist in allen USBSecure-Konfigurationsdateien nicht relevant. Eintrag VID_090C&PID_1000 und Eintrag Vid_090C&Pid_1000 gelten als identisch.

USB-Geräte pro Computer freigeben

Ab Version 4.4 ist es möglich, USB-Geräte auch „pro Computer" freizugeben. Das bietet sich an, wenn an einem bestimmten Computer, an dem sich mehrere Benutzer anmelden, ein spezielles USB-Gerät angeschlossen ist, das immer freigegeben sein soll. Verwenden Sie dafür folgende Notation:

```
[Host:<Computername>]
<erlaubtes Gerät>
```

Beispiel:

```
[Host:PC01234]
VID_090C&PID_1000
```

Die Einträge addieren sich, falls es sowohl für den Benutzer als auch für den Computer, an dem sich der Benutzer anmeldet, zutreffende Einträge gibt.

Services

Mit dem Service-Eintrag können komplette Geräteklassen freigegeben werden. Folgende Notation wird verwendet:

```
service = <Service-Name>
```

Beispiel: `service = usbstor`

Häufig verwendete Werte:

service=usbhub	USB-Root-Hubs
service=usbhub3	USB3-Root-Hubs
service= iusb3hub	USB3-Root-Hubs
service=hidusb	USB-Tastaturen und -Mäuse
service=usbstor	USB-Massenspeicher (Sticks, Festplatten…)
service=usbprint	USB-Drucker
service=usbscan	USB-Scanner

Die Zugehörigkeit eines USB-Gerätes zu einem Service finden Sie im Geräte-Manager / Eigenschaften des Gerätes / Details / Dienst.

Standardmäßig freigegebene Geräte

Ab USBSecure Professional Version 4.3 sind bestimmte USB-Geräte per default eingeschaltet, auch wenn sie nicht in der usb.cfg erscheinen. Es handelt sich um alle Geräte, die im Feld „Dienst" (Service) den Wert usbhub, usbhub3, iusb3hub oder hidusb aufweisen. Dadurch wird bei einer

Fehlkonfiguration der usb.cfg-Datei ein Totalausfall vermieden. Soll einer der Dienste trotzdem deaktiviert werden, lässt sich das mit folgender Notation im AllUsers-Bereich erreichen:

```
no-defaultservice = <Service-Name>
```

Beispiel: `no-defaultservice = hidusb`

Benutzer

Benutzer können in folgender Notation angegeben werden:

[domain\user] Domäne und Benutzer

[user@domain] Benutzer und Domäne

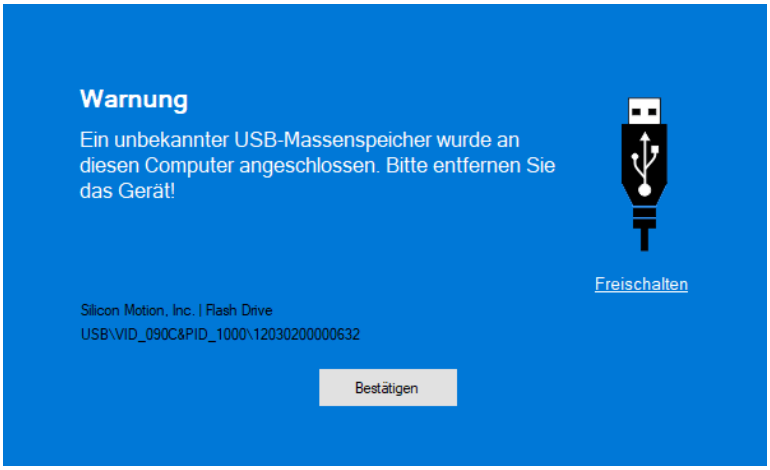
[user] Nur der Benutzer wird angegeben. Die Domäne ist hier beliebig. Die Einstellungen gelten dann für lokale und Domänenbenutzer, die dem **user** entsprechen.

Power User

PowerUser sind Benutzer, die die Berechtigung haben, USB-Massenspeicher (Sticks, Festplatten) temporär freizuschalten. Wird ein nicht erlaubter USB-Massenspeicher eingesteckt, erscheint beim Warnhinweis ein zusätzlicher Punkt „Freischalten“. Der Benutzer hat dann die Möglichkeit, den USB-Massenspeicher bis zum nächsten Neustart des USBSecure-Dienstes zu verwenden.

Verwenden Sie dazu folgende Notation:

```
[Benutzer]
>PowerUser
```



Blacklist-Services

Seit USBSecure Professional Version 3.3 kann in der usb.cfg mit Blacklists gearbeitet werden. Dadurch werden Konfigurationen wie *"Erlaube allen Benutzern alle USB-Geräte außer USB-Massenspeicher"* ermöglicht. Blacklist-Services werden in folgender Notation angegeben:

```
blacklist-service = <Service-Name>
```

Beispiel: `blacklist-service = usbstor`

Hinweis: Whitelists überschreiben Blacklists! Wenn ein Benutzer in seiner Konfiguration die Einträge **`blacklist-service = usbstor`** und **`service = usbstor`** hat, sind USB-Massenspeicher erlaubt.

Beispielkonfigurationen usb.cfg

Sie möchten...

...nur USB-Tastaturen und Mäuse erlauben, sonst nichts:

```
[AllUsers]
service = usbhub   # USB-Roothubs müssen immer erlaubt sein
service = usbhub3  # USB-Roothubs müssen immer erlaubt sein
service = hidusb   # alle USB-Tastaturen und -Mäuse erlaubt
```

...nur USB-Tastaturen und Mäuse erlauben, sonst nichts. Jedoch für Benutzer Müller zusätzlich einen bestimmten USB-Stick:

```
[AllUsers]
service = usbhub   # USB-Roothubs müssen immer erlaubt sein
service = usbhub3  # USB-Roothubs müssen immer erlaubt sein
service = hidusb   # alle USB-Tastaturen und -Mäuse erlaubt

[mueller]
VID_090C&PID_34C7  # hier die VidPid des Sticks eintragen, s. Geräte-Manager
```

...nur USB-Tastaturen und Mäuse erlauben, sonst nichts. Jedoch für Benutzer Schmidt zusätzlich alle USB-Massenspeicher:

```
[AllUsers]
service = usbhub   # USB-Roothubs müssen immer erlaubt sein
service = usbhub3  # USB-Roothubs müssen immer erlaubt sein
service = hidusb   # alle USB-Tastaturen und -Mäuse erlaubt

[schmidt]
service = usbstor  # USB-Massenspeicher
service = UASPStor # USB-Massenspeicher (neuere)
```

...nur USB-Tastaturen und Mäuse erlauben, sonst nichts. Jedoch für Benutzer Administrator alle USB-Geräte:

```
[AllUsers]
service = usbhub   # USB-Roothubs müssen immer erlaubt sein
service = usbhub3  # USB-Roothubs müssen immer erlaubt sein
service = hidusb   # alle USB-Tastaturen und -Mäuse erlaubt

[administrator]
*
```

...für alle Benutzer alle USB-Geräte erlauben, jedoch keine USB-Massenspeicher

```
[AllUsers]
*
blacklist-service = usbstor
blacklist-service = UASPStor
```

...für alle Benutzer alle USB-Geräte erlauben, jedoch keine USB-Massenspeicher. Für Benutzer Administrator alle USB-Massenspeicher erlauben und für Benutzer Meier nur einen bestimmten USB-Massenspeicher:

```
[AllUsers]
*
blacklist-service = usbstor
blacklist-service = UASPStor

[administrator]
service = usbstor   # USB-Massenspeicher
service = UASPStor  # USB-Massenspeicher (neuere)

[meier]
VID_090C&PID_34C7   # hier die VidPid des Sticks eintragen, s. Geräte-Manager
```

bluetooth.cfg

In der Datei ***bluetooth.cfg*** wird der Zugriff auf Bluetooth-Geräte geregelt. Analog zur Datei usb.cfg gibt es einen AllUsers-Bereich und einen Bereich pro Benutzer oder Computer:

```
[AllUsers]
…

[BenutzerA]
…

[BenutzerB]
…

[host:PC12345]
…
```

Wie in der Datei usb.cfg ist es möglich, Bluetooth-Geräte pro Benutzer und pro Computer freizugeben. Auch das Freigeben von Services ist möglich. Allerdings gibt es keine Blacklist-Services und keine PowerUser, dafür aber die Einträge AllowFiletransfer und AllowPanNetwork.

AllowFiletransfer

Verwenden Sie AllowFiletransfer=no, um den Transfer von Dateien und Ordnern über Bluetooth zu unterbinden. Eine Datei lässt sich über Bluetooth zwischen zwei gekoppelten Geräten übertragen, indem man mit rechter Maustaste auf die Datei klickt → Senden an → Bluetooth-Gerät. Durch AllowFiletransfer=no wird das Bluetooth-Gerät „Bluetooth Device (RFCOMM Protocol TDI)“ deaktiviert, wodurch kein Dateitransfer mehr möglich ist.
Bitte beachten: AllowFiletransfer=yes „schlägt“ AllowFiletransfer=no. Dadurch ist es möglich, den Dateitransfer grundsätzlich zu unterbinden (AllowFiletransfer=no im AllUsers-Bereich) und nur für einzelne Benutzer zu erlauben (AllowFiletransfer=yes im Benutzer-Bereich).

AllowPanNetwork

Verwenden Sie AllowPanNetwork=no, um die Teilnahme an einem PAN-Netzwerk (Personal Area Network) über Bluetooth zu unterbinden. Bei einem PAN-Netzwerk handelt es sich um ein drahtloses Netzwerk über die Bluetooth-Schnittstelle. Es lässt sich ganz einfach einrichten, indem man auf das Bluetooth-Icon im Systemtray klickt → „Einem persönlichen Netzwerk beitreten“. Durch AllowPanNetwork=no wird die virtuelle Netzwerkkarte „Bluetooth-Gerät (PAN)“ deaktiviert, wodurch die Erstellung eines PAN-Netzwerks nicht mehr möglich ist.
Bitte beachten: AllowPanNetwork=yes „schlägt“ AllowPanNetwork=no. Dadurch ist es möglich, die Einrichtung von PAN-Netzwerken grundsätzlich zu unterbinden (AllowPanNetwork=no im AllUsers-Bereich) und nur für einzelne Benutzer zu erlauben (AllowPanNetwork=yes im Benutzer-Bereich).

Alle Bluetooth-Einstellungen werden erst dann wirksam, wenn eine funktionsfähige Bluetooth-Schnittstelle vorliegt. Bei der Bluetooth-Schnittstelle selbst handelt es sich meistens um ein USB-Gerät, das somit in der Datei usb.cfg freigeschaltet werden muss.

Bluetooth-Konfigurationsbeispiel 1: Alle Bluetooth-Geräte erlauben, Dateitransfer verbieten

Eine Information vorab: Die Freigabe von Bluetooth-Geräten ist komplizierter als die Freigabe von USB-Geräten. Während es bei USB-Geräten in den meisten Fällen genau einen Eintrag im Gerätemanager für ein Gerät gibt, ist es bei Bluetooth meistens notwendig, mehrere virtuelle Geräte freizuschalten, um ein reales Gerät verwenden zu können.
Aus diesem Grund ist genau dieses Konfigurationsbeispiel sehr interessant. Es verbietet Dateitransfer über Bluetooth – bei geringstem administrativen Aufwand.

Ziel in diesem Beispiel ist es, grundsätzlich alle Bluetooth-Geräte zu erlauben, jedoch Dateitransfer über Bluetooth zu unterbinden.

Sorgen Sie zunächst dafür, dass Ihre Bluetooth-Schnittstelle funktioniert. In vielen Fällen muss dafür ein USB-Gerät freigeschaltet werden – die eigentliche Bluetooth-Schnittstelle. Das Gerät könnte zum Beispiel „Intel® Wireless BlueTooth®“ oder „Broadcom Bluetooth Adapter“ heißen.

Der AllUsers-Bereich der Datei bluetooth.cfg sieht im Standard folgendermaßen aus:

```
[AllUsers]
*
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
```

► Schritt 1: Ändern des Eintrags, der den Dateitransfer von Dateien und Ordnern erlaubt:

```
AllowFiletransfer=no
```

Durch diesen Eintrag wird der Dateitransfer über *rechte Maustaste → Senden an → Bluetooth-Gerät* und über *Klick auf das Bluetooth-Icon im Systemtray → Datei senden* unterbunden.

► Schritt 2: Ändern des Eintrags, der das Erstellen von PAN-Netzwerken erlaubt:

```
AllowPanNetwork=no
```

Durch diesen Eintrag wird das Einrichten und die Teilnahme an einem PAN (Personal Area Network) über Bluetooth unterbunden.

Wir erhalten folgenden AllUsers-Bereich:

```
[AllUsers]
*
AllowFiletransfer=no
```

```
AllowPanNetwork=no
service=UmPass
```

Mit dieser Konfiguration werden das virtuelle Bluetooth-Gerät „Bluetooth Device (RFCOMM Protocol TDI)“ und die virtuelle Netzwerkkarte „Bluetooth-Gerät (PAN)“ deaktiviert. Das Ziel wird erreicht, alle Bluetooth-Geräte zu erlauben, jedoch Dateitransfer über Bluetooth zu unterbinden.

Möchten Sie Dateitransfer für einzelne Benutzer oder Computer ermöglichen, können Sie im Bereich des Benutzers oder Computers den jeweiligen Eintrag mit „yes“ verwenden („yes“ überschreibt „no“):

```
[MuellerM]
AllowFiletransfer=yes
```

oder

```
[host:PC12345]
AllowFiletransfer=yes
```

Bluetooth-Konfigurationsbeispiel 2: Erlauben einer Bluetooth-Maus

Ziel in diesem Beispiel soll es sein, die Microsoft Bluetooth Mouse 3600 für alle Benutzer freizuschalten – alle anderen Bluetooth-Geräte sollen verboten sein. Das Beispiel ist auf jede andere Bluetooth-Maus übertragbar.

Sorgen Sie zunächst dafür, dass Ihre Bluetooth-Schnittstelle funktioniert. In vielen Fällen muss dafür ein USB-Gerät freigeschaltet werden – die eigentliche Bluetooth-Schnittstelle. Das Gerät könnte zum Beispiel „Intel® Wireless BlueTooth®“ oder „Broadcom Bluetooth Adapter“ heißen.

Der AllUsers-Bereich der Datei bluetooth.cfg sieht im Standard folgendermaßen aus:

```
[AllUsers]
*
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
```

► Schritt 1: Entfernen des Sterns (*), der alle Bluetooth-Geräte für alle Benutzer freischaltet. Wir erhalten dann folgenden AllUsers-Bereich:

```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
```

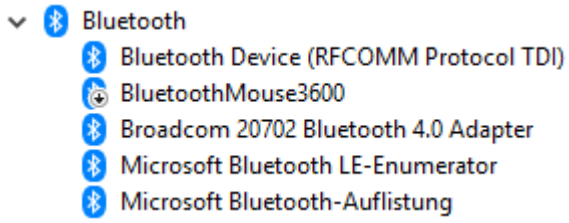
Achtung: Falls Sie diesen Schritt in Ihrer produktiven Umgebung durchführen, werden Bluetooth-Geräte nicht mehr funktionieren!

► Schritt 2: Sorgen Sie dafür, dass die Geräte „Microsoft Bluetooth LE-Enumerator“ und „Microsoft Bluetooth-Auflistung“ aktiviert sind, indem Sie jeweils den Geräteinstanzpfad im AllUsers-Bereich eintragen. Verwenden Sie nur den vorderen Teil, um diese beiden Geräte netzwerkweit freizugeben:

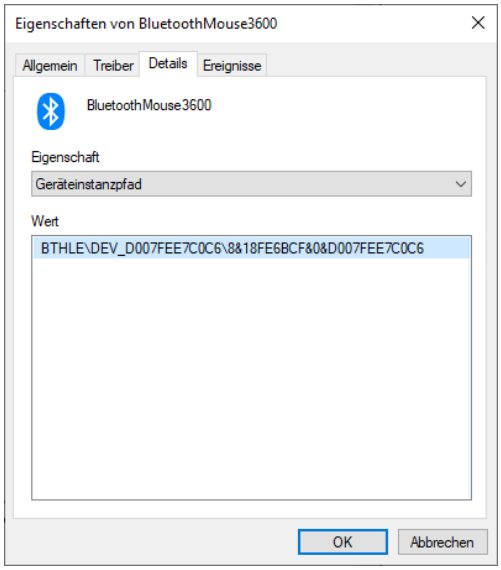
```
BTH\MS_BTHLE
BTH\MS_BTHBRB
```

Starten Sie den USBSecure-Dienst neu, so dass die Einstellungen wirken.

► Schritt 3: Koppeln Sie die Bluetooth-Maus mit dem Computer über Einstellungen → Bluetooth- und andere Geräte. Sie wird nach dem Verbinden deaktiviert.



► Schritt 4: Eintragen des Geräteinstanzpfades des Gerätes „BluetoothMouse3600“ aus dem Gerätemanager in den AllUsers-Bereich:

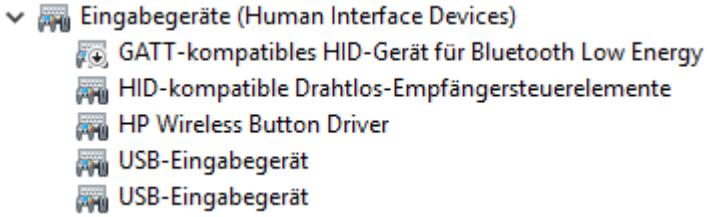


Der AllUsers-Bereich sieht jetzt so aus (der Eintrag für die Maus kann abweichen):

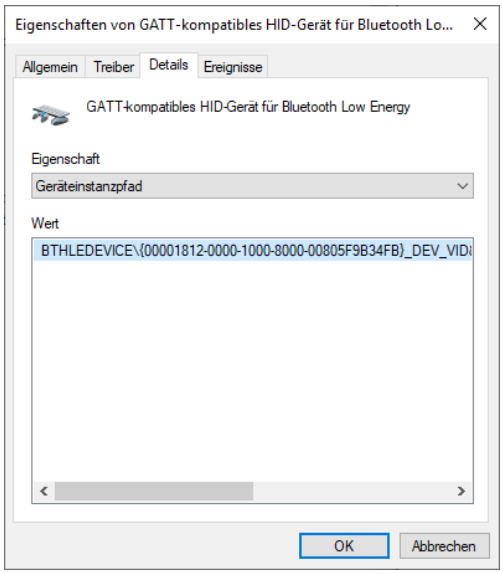
```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
BTH\MS_BTHLE
BTH\MS_BTHBRB
BTHLE\DEV_D007FEE7C0C6\8&18FE6BCF&0&D007FEE7C0C6
```

Das Gerät „BluetoothMouse3600“ wird nach Neustart des USBSecure-Dienstes eingeschaltet. Trotzdem funktioniert die Maus noch nicht.

Unter „Eingabegeräte“ befindet sich noch ein Gerät, das eingeschaltet werden muss:



► Schritt 4: Eintragen des Geräteinstanzpfades des Gerätes „GATT-kompatibles HID-Gerät für Bluetooth Low Energy“ aus dem Gerätemanager in den AllUsers-Bereich.



Es wird nur der feststehende vordere Teil des Geräteinstanzpfades eingetragen, so dass alle Geräte des gleichen Typs freigeschaltet sind:

```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
BTH\MS_BTHLE
BTH\MS_BTHBRB
BTHLE\DEV_D007FEE7C0C6\8&18FE6BCF&0&D007FEE7C0C6
BTHLEDEVICE\{00001812-0000-1000-8000-00805F9B34FB}_DEV_VID&02045E_PID&0916_REV&0110
```

BluetoothMouse3600 wird nach Neustart des USBSecure-Dienstes eingeschaltet und funktioniert.

► Problem: Der Geräteinstanzpfad des Gerätes BluetoothMouse3600 ist sehr variabel. Selbst nach Entfernen und Wiederverbinden (Koppeln) der Maus ändert sich der Geräteinstanzpfad:

vorher:

```
BTHLE\DEV_D007FEE7C0C6\8&18FE6BCF&0&D007FEE7C0C6
```

nachher:

```
BTHLE\DEV_D008FCE8C0C6\8&18FE6BCF&0&D008FCE8C0C6
```

Das Problem ließe sich mit folgendem Eintrag lösen:

```
BTHLE\DEV_D00?F?E?C0C6\8&18FE6BCF&0&D00?F?E?C0C6
```

Ein Fragezeichen steht für ein Zeichen. Gelöst wäre allerdings nur das Problem für diese bestimmte Maus. Eine weitere baugleiche Maus kann einen komplett anderen Geräteinstanzpfad aufweisen.

► Lösung: In der Datei bluetooth.cfg können Anzeigenamen verwendet werden. Dabei handelt es sich um die Namen, die Im Gerätemanager zu sehen sind. In unserem Fall lautet der Anzeigename „BluetoothMouse3600“. Die komplette bluetooth.cfg sieht damit folgendermaßen aus:

```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
BTH\MS_BTHLE
BTH\MS_BTHBRB
BluetoothMouse3600
BTHLEDEVICE\{00001812-0000-1000-8000-00805F9B34FB}_DEV_VID&02045E_PID&0916_REV&0110
```

Bitte beachten Sie, dass nicht alle Anzeigenamen verwendet werden können. Um eine Liste mit verwendbaren Anzeigenamen zu erhalten, führen Sie bitte die VBS-Datei ShowBluetoothDisplaynames.vbs im USBSecure-Verzeichnis aus.

Bluetooth-Konfigurationsbeispiel 3: Erlauben eines SmartPhones

Ziel in diesem Beispiel soll es sein, ein bestimmtes SmartPhone (Android oder iPhone) für den AD-Benutzer MuellerM freizuschalten. Die Verbindung soll über Bluetooth erfolgen – alle anderen Bluetooth-Geräte sollen verboten sein.

Sorgen Sie zunächst dafür, dass Ihre Bluetooth-Schnittstelle funktioniert. In vielen Fällen muss dafür ein USB-Gerät freigeschaltet werden – die eigentliche Bluetooth-Schnittstelle. Das Gerät könnte zum Beispiel „Intel® Wireless BlueTooth®“ oder „Broadcom Bluetooth Adapter“ heißen.

Die Konfigurationsdatei bluetooth.cfg sieht im Standard folgendermaßen aus:

```
[AllUsers]
*
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
```

► Schritt 1: Entfernen des Sterns (*), der alle Bluetooth-Geräte für alle Benutzer freischaltet. Wir erhalten dann folgenden AllUsers-Bereich:

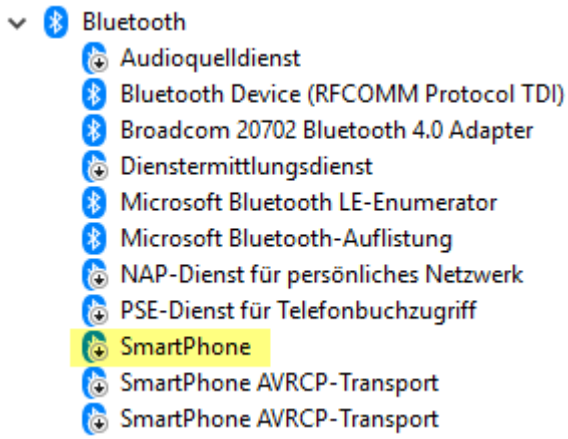
```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
```

Achtung: Falls Sie diesen Schritt in Ihrer produktiven Umgebung durchführen, werden Bluetooth-Geräte nicht mehr funktionieren!

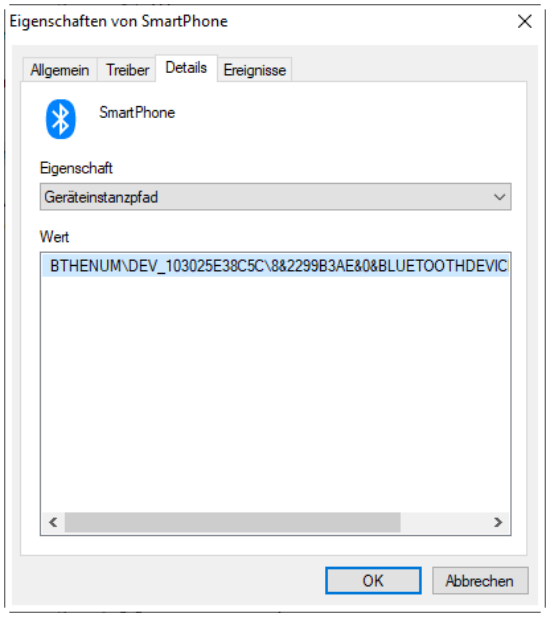
Hinweis: Mit dieser Konfiguration würde ein neu angeschlossenes SmartPhone im Gerätemanager als „deaktiviert“ angezeigt werden. Der Dateitransfer über die Bluetooth-Schnittstelle wäre durch die vorhandene Einstellung `AllowFiletransfer=yes` trotzdem möglich.

► Schritt 2: Verbinden des SmartPhones über Einstellungen → Bluetooth- und andere Geräte

Das SmartPhone wird nach dem Verbinden als deaktiviert angezeigt.



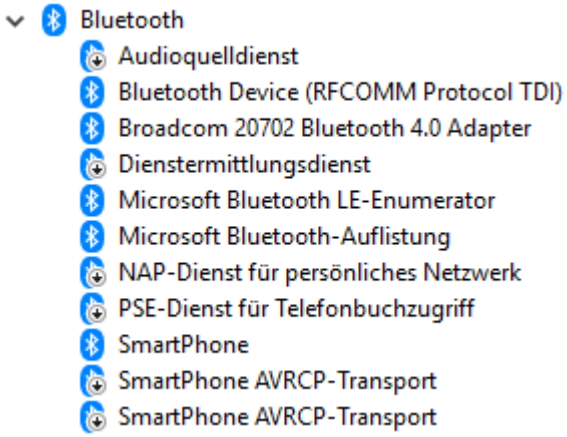
► Schritt 3: Eintragen des Geräteinstanzpfades des Gerätes „SmartPhone“ aus dem Gerätemanager in den Bereich für Benutzer MuellerM:



Die Datei bluetooth.cfg sieht jetzt so aus:

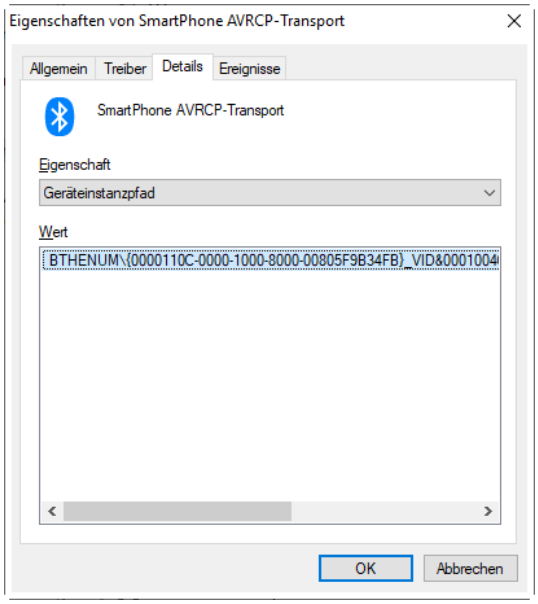
```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass

[MuellerM]
BTHENUM\DEV_103025E38C5C\8&2299B3AE&0&BLUETOOTHDEVICE_103025E38C5C
```

Das Gerät „SmartPhone“ wird nach Neustart des USBSecure-Dienstes eingeschaltet. Allerdings gibt es noch einige deaktivierte Geräte:



Jetzt müssten die Geräteinstanzpfade aller deaktivierten Geräte für MuellerM eingetragen werden. Es gibt aber auch einen einfacheren Weg:

Wir benötigen den Geräteinstanzpfad eines der deaktivierten Geräte, zum Beispiel den des Gerätes „SmartPhone AVRCP-Transport“.



Beim Vergleich der Geräteinstanzpfade aller noch deaktivierten Geräte fällt auf, dass sie sich nur unwesentlich voneinander unterscheiden. Wir ersetzen die sich unterscheidenden Ziffern durch Fragezeichen:

```
BTHENUM\{????????????????????????????????????}_VID&0001004C_PID&7003\8&2299B3AE&
0&103025E38C5C_C00000000
```

► Schritt 4: Eintragen des variablen Geräteinstanzpfades für alle noch deaktivierten Geräte:

```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass

[MuellerM]
BTHENUM\DEV_103025E38C5C\8&2299B3AE&0&BLUETOOTHDEVICE_103025E38C5C
```

```
BTHENUM\{????????????????????????????????????}_VID&0001004C_PID&7003\8&2299B3AE&
0&103025E38C5C_C00000000
```

Das SmartPhone wird nach Neustart des USBSecure-Dienstes eingeschaltet und funktioniert.

Um die Dateiübertragung via SmartPhone ausschließlich Benutzer MuellerM zu erlauben und allen anderen Benutzern zu verbieten, ist folgende Konfiguration erforderlich:

```
[AllUsers]
AllowFiletransfer=no
AllowPanNetwork=no
service=UmPass

[MuellerM]
AllowFiletransfer=yes
AllowPanNetwork=yes
BTHENUM\DEV_103025E38C5C\8&2299B3AE&0&BLUETOOTHDEVICE_103025E38C5C
BTHENUM\{????????????????????????????????????}_VID&0001004C_PID&7003\8&2299B3AE&
0&103025E38C5C_C00000000
```

Die Dateiübertragung ist damit grundsätzlich unterbunden und nur für Benutzer MuellerM erlaubt.

USBSecure.ini

In der Datei USBSecure.ini werden PC-bezogene, allgemeine Einstellungen vorgenommen. Im Standardfall muss diese Datei nicht modifiziert werden.

Server = <Name des USBSecure-Servers>

Hier wird der USBSecure-Server angegeben. Es handelt sich dabei um den Server mit der devices$-Freigabe (s. Installation des Servers)

LogLevel=<normal|full>

Bestimmt die Ausführlichkeit der Protokollierung in die Datei USBSecure.log. Im Produktivbetrieb sollte diese Einstellung auf „normal“ stehen. Für ausführlicheres Logging kann „full“ eingestellt werden.

ViolationReboot=<yes|no>

Definiert das Verhalten bei Geräten, die vom Betriebssystem nicht ohne Reboot deaktiviert werden können, weil sie sich im Zugriff befinden. ViolationReboot=yes bedeutet, dass ein Reboot durchgeführt werden soll.

RebootDelay=60

RebootDelay gibt die Verzögerung (in Sek.) an, d.h. die Zeit, die dem Benutzer bleibt, bis der Rechner durchgestartet wird.

RebootMessage=Unregistriertes USB-, CD- oder Diskettenlaufwerk entdeckt...

Die Meldung, die der Benutzer vor dem Reboot erhält.

ViolationEject=<yes|no>

Gibt an, ob ein Wechseldatenträger (USB-Stick, CD, …), der nicht vom Betriebssystem deaktiviert werden kann (z.B. weil er sich im Zugriff befindet), ausgeworfen wird. Ein ausgeworfenes Gerät muss neu eingesteckt werden, um bei zugelassenen Benutzern zu funktionieren.

ScsiSupport=<yes|no>

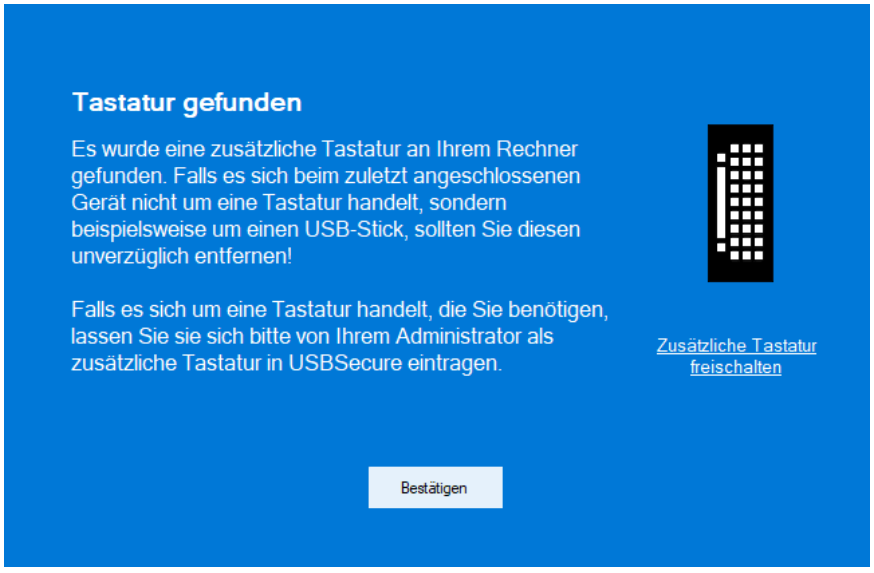
Gibt an, ob SCSI CD-Laufwerke unterstützt werden sollen.

UsbLoggedOffDeactivation=<yes|no>

Per Default werden alle USB-Geräte, die nicht im AllUsers-Bereich der Datei usb.cfg aufgeführt sind, im abgemeldeten Zustand (Windows Logoff) deaktiviert. Dies geschieht sowohl beim echten „Abmelden“ als auch beim Hochfahren eines Rechners (vor der Anmeldung) und beim Herunterfahren. In Einzelfällen ist dieses Verhalten unerwünscht. Beispielsweise könnte es sein, dass ein USB-Fotoapparat beim Herunterfahren des Rechners eingesteckt war und dadurch deaktiviert wird. Wird er dann abgezogen und später nach der Windows-Anmeldung wieder eingesteckt, wird er in manchen Fällen nicht aktiviert. Verwenden Sie dann „UsbLoggedOffDeactivation=no“. Diese Einstellung hat den Effekt, dass USB-Geräte tatsächlich nur dann deaktiviert werden, wenn sich ein Benutzer ohne Berechtigung für das Gerät anmeldet (und nicht bei jeder Abmeldung).

KeyboardInstall=<block|warn|allow> (default: warn)

Durch manipulierte USB-Sticks, die sich beispielsweise als USB-Tastaturen ausgeben, können von Angreifern unerwünschte Manipulationen an Rechnern vorgenommen werden (BadUSB). USBSecure ermittelt beim allerersten Starten des USBSecure-Dienstes die Anzahl der angeschlossenen Tastaturen (sofern KeyboardInstall=block oder KeyboardInstall=warn eingestellt ist) und schreibt den Wert in die Datei KeyboardCount.cfg. Wird irgendwann eine zusätzliche Tastatur angeschlossen, wird der Rechner gesperrt und der Anwender erhält einen Warnhinweis mit einer Erklärung. Im Modus **KeyboardInstall=warn** bleibt es beim Warnhinweis. Falls es sich um eine echte Tastatur handelt, kann Sie nach Bestätigung durch den Benutzer verwendet werden. Der Benutzer hat außerdem die Möglichkeit, die Anzahl erlaubter Tastaturen selbständig zu erhöhen. Im Modus **KeyboardInstall=block** wird der Rechner immer wieder sofort gesperrt, solange die zusätzliche Tastatur angeschlossen ist. Erst nach Entfernen des Gerätes ist der Rechner wieder verwendbar.



Das Freischalten einer zusätzlichen Tastatur für einen Anwender erfolgt über die lokale Datei KeyboardCount.cfg (im USBSecure-Verzeichnis). Erhöhen Sie dort den Wert manuell oder löschen Sie die Datei und starten Sie den USBSecure-Dienst neu. Wichtig: in der Datei USBSecure.ini muss KeyboardInstall=warn oder KeyboardInstall=block definiert sein – nur dann erscheint diese Meldung. Bei KeyboardInstall=warn kann der Benutzer die Tastatur selbständig freischalten. Der Text ist frei konfigurierbar, s.unten (TextKeyboardWarning).

LocalDevicesCopy=30

Gibt an, ob die Textdateien mit installierten USB-Geräten aller Benutzer zentral abgelegt werden sollen. Die Read/Write-Freigabe devicesRW$ mit Verzeichnis ExistingUsbDevices muss dafür existieren (Wert in Minuten, 0=nie). Die Dateien werden nach \\devicesRW$\ExistingUsbDevices kopiert.

IniOverwrite=60

Steuert die zentrale Verwaltung der USBSecure.ini. Gibt an, ob die Datei USBSecure.ini von der zentralen USBSecure.ini (in devices$) überschrieben werden soll (in Minuten, 0=nie). Bleibt wirkungslos, falls keine zentrale USBSecure.ini vorhanden ist.
Mit diesem Eintrag ist es auch möglich, unterschiedliche Sprachen für die USBSecure-Dialoge (unbekannter Massenspeicher und neue Tastatur) zu implementieren. Je nach Betriebssystemsprache wird eine unterschiedliche USBSecure.ini von der zentralen devices$ ins lokale USBSecure-Verzeichnis kopiert. Innerhalb der USBSecure.ini-Datei lassen sich Texte für die Dialoge definieren (s.u.). Der Name der zentralen USBSecure.ini-Datei muss folgendermaßen lauten: USBSecureLanguage<InstallLanguage>.ini. Der Wert für <InstallLanguage> entspricht dem Registry-Wert InstallLanguage unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language. Für ein deutsches Betriebssystem lautet der Name der Datei dann USBSecureLanguage0407.ini.

Ein Beispiel: Sie haben in Ihrem Unternehmen deutsche, englische und französische Clients und möchten die USBSecure-Dialoge der jeweiligen Landessprache anpassen. Setzen Sie dazu IniOverwrite auf 5 – dies kann auch schon während der Installation über MSI-Parameter erfolgen. Erstellen Sie folgende Dateien in der zentralen Freigabe \\<IhrServer>\devices$: USBSecureLanguage0407.ini, USBSecureLanguage0409.ini und USBSecureLanguage040c.ini. Als Vorlage nehmen Sie dafür die Datei USBSecure.ini aus Ihrer lokalen Installation (C:\Program Files (x86)\USBSecure). Erstellen Sie deutsche Dialogtexte (z.B. TextUsbWarning1, s.u.) in der Datei USBSecureLanguage0407.ini, englische Texte in der Datei USBSecureLanguage0409.ini und französische Texte in der Datei USBSecureLanguage040c.ini. Die jeweiligen .ini-Dateien werden 5 Minuten nach Start des USBSecure-Dienstes (bei IniOverwrite=5) von der zentralen Freigabe als USBSecure.ini in das lokale USBSecure-Verzeichnis kopiert. Somit erhalten Ihre Anwender angepasste Dialoge.

Sind keine landesspezifischen USBSecure.ini-Dateien in devices$ vorhanden, wird die Datei USBSecure.ini herangezogen. Ist auch diese nicht vorhanden, passiert gar nichts.
.

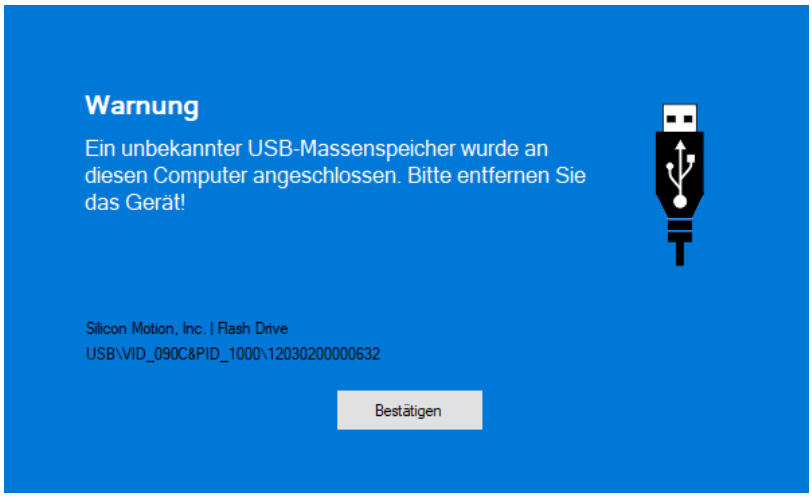
Backup=60

Macht den lokalen Rechner zum USBSecure-Sicherungsrechner. Alle .cfg-Dateien und die USBSecure.ini werden alle 60 Minuten (Wert in Minuten, 0=nie) von der devices$-Freigabe auf den lokalen Rechner ins Unterverzeichnis **backup** kopiert. Jede Datei erhält dabei einen Zeitstempel im Dateinamen – alte Stände werden nicht überschrieben.

NoUsbStorInfo=<yes|no|warn> (default: no)

Im Default wird ab USBSecure Professional 3.4 bei Einstecken eines verbotenen USB-Massenspeichers ein Warnhinweis ausgegeben und der Rechner gesperrt. Bei NoUsbStorInfo=yes erfolgt (wie bis Version 3.3) keine Information und keine Sperrung des Rechners. Bei NoUsbStorInfo=no (default) wird ein Info-Fenster eingeblendet und der Rechner wird gesperrt. Der Benutzer kann sich dann sofort wieder anmelden. Der Warnhinweis erscheint nur, wenn ein USB-Massenspeicher im laufenden Betrieb eingesteckt wird. Ein verbotener USB-Massenspeicher, der beim Booten bereits eingesteckt ist, wird ohne Warnhinweis deaktiviert.
Diesen Wert können Sie während der unbeaufsichtigten Installation mit angeben. Falls das Default-Verhalten (Einblendung des Warnhinweises) nicht erwünscht ist, können Sie als zusätzliche MSI-Variable NOUSBSTORINFO=yes angeben.

Bei **NoUsbStorInfo=warn** wird der blaue Warnhinweis eingeblendet, der Rechner jedoch nicht gesperrt.



Der Text ist frei konfigurierbar, s.unten (TextUsbWarning).

ForceUsbstorUnplug=<yes|no> (default: no)

Bei USB-Massenspeichern, die sich unter ungünstigen Bedingungen nicht deaktivieren lassen, wird der Computer durch **ForceUsbstorUnplug=yes** mit einer ca. 20 Sekunden dauernden Verzögerung immer wieder gesperrt, bis der USB-Massenspeicher entfernt wurde.

ResolveVendors=<yes|no> (default: yes)

ResolveVendors gibt an, ob im Logfile USBSecure.log Hersteller der Geräte anhand der Datei vendors.txt ermittelt werden sollen.

SmartphoneInfo=<yes|no> (default: no)
Bei SmartphoneInfo=yes wird auch bei Smartphones, Kameras und ähnlichem der blaue Warnhinweis eingeblendet. Im Standard passiert dies nur bei USB-Massenspeichern, die dem Dienst USBSTOR angehören. Genauer gesagt wird bei SmartphoneInfo=yes der Warnhinweis immer dann eingeblendet, wenn ein nicht erlaubtes USB-Gerät angeschlossen wird, das im Feld Dienst (s. Gerätemanager oder DeviceTool) den Wert WUDFrd (z.B. Apple iPhone) oder den Wert WUDFWpdMtp (z.B. Android-Smartphones) aufweist.

Windows7Mode=<yes|no> (default: no)

In früheren USBSecure-Versionen wurden unter Windows 7 (und Windows XP) nur USB-Geräte deaktiviert, die tatsächlich eingeschaltet waren. Dies geschah aus Performance-Gründen und war bei alten, extrem langsamen Rechnern sinnvoll. Ab Windows 8 funktioniert die einfache Erkennung (ob ein- oder ausgeschaltet) nicht mehr in jedem Fall, so dass immer alle nicht erlaubten USB-Geräte deaktiviert werden – nicht nur die tatsächlich eingeschalteten. Setzen Sie **Windows7Mode=yes**, um das alte Verfahren zu verwenden.

UsbStorNotify=<yes|no> (default: no)

Mit **UsbStorNotify=yes** wird beim Einstecken eines unbekannten USB-Massenspeichers (Stick, Festplatte) eine Datei in der Freigabe devicesRW$\Notify erzeugt, die dann beispielsweise mit dem

mitgelieferten SmtpSend.exe weiterverarbeitet werden kann. Die Freigabe devicesRW$\Notify muss dafür existieren.

UsbCfgSizeCheck=<yes|no> (default: yes)

Ab Version 4.3 wird jede neue usb.cfg-Datei, die vom Server auf den Client kopiert wird, auf Plausibilität bzgl. der Dateigröße überprüft. Ist die usb.cfg kleiner 15 Byte groß oder kleiner als 50% der Vorgängerversion (aber mindesten 1500 Byte groß), kommt sie nicht zum Einsatz. Stattdessen wird dann die Vorgängerversion aus dem lokalen Unterverzeichnis „cache“ verwendet. Dadurch werden versehentliche Fehlkonfigurationen entschärft. Bei UsbCfgSizeCheck=no findet keine Überprüfung statt.

SmtpServer=<Name des Mailservers>
MailFrom=<Absendername>
MailTo1=<Empfängername1>
MailTo2=<Empfängername2>
MailTo3=<Empfängername3>

Tragen Sie hier ein, wer benachrichtigt werden soll, wenn ein unbekannter USB-Massenspeichers eingesteckt wurde. Zumindest die Werte SmtpServer, MailFrom und MailTo1 müssen gesetzt werden. Diese Einstellungen sind unabhängig vom Wert, der bei UsbStorNotify gesetzt wurde. Es handelt sich dabei um zwei alternative Benachrichtigungsmethoden.

Definieren Sie eigene Texte, die beim Einstecken eines unbekannten USB-Massenspeichers erscheinen sollen. „\n“ für Zeilenumbruch:

TextUsbWarning1=Warnung
TextUsbWarning2=Ein unbekannter USB-Massenspeicher wurde an diesen Computer angeschlossen. Bitte entfernen Sie das Gerät!
TextUsbUnlockLink=Freischalten
TextUsbConfirmButton=Bestätigen
TextUsbUnlock1=Sie haben die Möglichkeit, diesen USB-Massenspeicher temporär freizuschalten.\n\nHinweis: Die Freischaltung wird protokolliert.\n\nSoll der Massenspeicher jetzt freigeschaltet werden?
TextUsbUnlock2=Das Gerät wurde freigeschaltet. Möglicherweise muss es einmal vom Computer entfernt und neu eingesteckt werden.
TextUsbMsg=Ihr Rechner wurde aufgrund eines unbekannten USB-Massenspeichers gesperrt.\n\nBitte entfernen Sie das USB-Gerät und melden Sie sich erneut an.

Mit den beiden folgenden Variablen können Sie einen Link einblenden, um beispielsweise weitere Informationen zu Ihrer USB-Policy anzuzeigen. Beim Klick auf den Link wird die hinterlegte URL im Standardbrowser aufgerufen:

TextUsbLink=Weitere Informationen
UsbLink=http://intranet.meinefirma.de/usb

Definieren Sie eigene Texte, beim Anschließen einer zusätzlichen Tastatur erscheinen sollen. „\n“ für Zeilenumbruch:

TextKeyboardWarning1=Tastatur gefunden
TextKeyboardWarning2=Es wurde eine zusätzliche Tastatur an Ihrem Rechner gefunden. Falls es sich beim zuletzt angeschlossenen Gerät nicht um eine Tastatur handelt, sondern beispielsweise um einen USB-Stick, sollten Sie diesen unverzüglich entfernen!\n\nFalls es sich um eine Tastatur handelt, die Sie benötigen, lassen Sie sie sich bitte von Ihrem Administrator als zusätzliche Tastatur in USBSecure eintragen.

TextKeyboardUnlockLink=Zusätzliche Tastatur freischalten
TextKeyboardConfirmButton=Bestätigen
TextKeyboardUnlock=Sie haben die Möglichkeit, eine zusätzliche Tastatur freizuschalten.\n\nSoll die Tastatur jetzt freigeschaltet werden?
TextKeyboardMsg=Ihr Rechner wurde aufgrund einer zusätzlich angeschlossenen Tastatur gesperrt.\n\nHinweis: USB-Tastaturen, getarnt als USB-Sticks, können auf Ihrem Rechner und im Netzwerk Schaden anrichten.

Mit den beiden folgenden Variablen können Sie einen Link einblenden, um beispielsweise weitere Informationen zum Thema BadUSB anzuzeigen. Beim Klick auf den Link wird die hinterlegte URL im Standardbrowser aufgerufen:

TextKeyboardLink=Weitere Informationen
KeyboardLink=http://intranet.meinefirma.de/BadUsb

InstallLanguage=0407

Die Betriebssystemsprache wird vom USBSecure-Dienst automatisch erkannt – anhand des Registry-Eintrages InstallLanguage unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language. Der Wert hinter InstallLanguage= in der Datei USBSecure.ini überschreibt diesen Wert.

AdminsCantStop=<yes|no>

Gibt an, ob Administratoren das Recht haben, den USBSecure-Dienst zu beenden. Dieser Wert kann auch bereits während der Installation in der GUI oder per MSI-Variable (ADMINSCANTSTOP=1 oder 0) festgelegt werden. Bitte beachten Sie, dass sich eine Änderung dieses Wertes per USBSecure.ini erst 5 Minuten nach Dienststart auswirkt.
Grundsätzlich kann ein Administrator natürlich immer einen Dienst beenden. Im Zweifelsfall muss er sich die notwendigen Rechte dazu verschaffen. Durch diese Einstellung wird es einem Benutzer, der Administratoren-Rechte besitzt, etwas erschwert.

ApplyConfigAfterServiceStartup=<Zeit in Minuten>

Durch den Eintrag ApplyConfigAfterServiceStartup=5 wird die komplette Geräte-Konfiguration (usb.cfg, cd.cfg usw.) 5 Minuten nach Start des USBSecure-Dienstes neu vom Server kopiert und angewendet. Sinnvoll in Umgebungen, in denen das Netzwerk beim Dienststart eventuell nicht zur Verfügung steht, zum Beispiel in NAC-Umgebungen (Network Access Control). Mögliche Werte sind: 2 - 999 (0 = aus).

ApplyConfigDailyAt=<Uhrzeit>

Der Eintrag ApplyConfigDailyAt=00:30 sorgt dafür, dass die komplette Geräte-Konfiguration (usb.cfg, cd.cfg usw.) um 00:30 Uhr neu vom Server kopiert und angewendet wird. Sinnvoll in Umgebungen, in denen bestimmte Rechner 7x24 Stunden laufen. Falls der Rechner um 00:30 Uhr keine Netzwerkverbindung hat oder ausgeschaltet ist, wird der Vorgang nicht nachgeholt.

BluetoothSupport=<yes|no>

Der Eintrag BluetoothSupport=no sorgt dafür, dass die Ein- und Ausschaltung von Bluetooth-Geräten nicht unterstützt wird.

Beispielkonfigurationen USBSecure.ini

1. Sie möchten, dass bei eingesteckten USB-Massenspeichern, die nicht über die Datei usb.cfg freigegeben sind, der blaue Warnhinweis erscheint und der Rechner gesperrt wird (der Anwender kann sich sofort wieder anmelden). Unbekannte Smartphones und Digitalkameras sollen ohne Benachrichtigung gesperrt werden.

   Konfigurieren Sie dafür folgende Werte in der USBSecure.ini:

   → NoUsbStorInfo=no
   → SmartphoneInfo=no

2. Sie möchten, dass bei eingesteckten USB-Massenspeichern, die nicht über die Datei usb.cfg freigegeben sind, der blaue Warnhinweis erscheint, der Rechner aber nicht gesperrt wird. Unbekannte Smartphones und Digitalkameras sollen ohne Benachrichtigung gesperrt werden.

   Konfigurieren Sie dafür folgende Werte in der USBSecure.ini:

   → NoUsbStorInfo=warn
   → SmartphoneInfo=no

3. Sie möchten, dass bei eingesteckten USB-Massenspeichern, die nicht über die Datei usb.cfg freigegeben sind, der blaue Warnhinweis erscheint, der Rechner aber nicht gesperrt wird. Das gleiche soll bei unbekannten Smartphones und Digitalkameras geschehen.

   Konfigurieren Sie dafür folgende Werte in der USBSecure.ini:

   → NoUsbStorInfo=warn
   → SmartphoneInfo=yes

Mail-Benachrichtigung

Als USBSecure-Administrator Sie haben die Möglichkeit, sich per Mail benachrichtigen zu lassen, wenn ein unerlaubter USB-Massenspeicher (USB-Stick, USB-Festplatte) eingesteckt wurde. Da USBSecure keine echte Serverkomponente besitzt, muss der Mailversand direkt vom Client oder über einen zentralen geplanten Task (Aufgabe) erfolgen. Dafür gibt es zwei alternative Verfahren:

Direkter Mailversand vom Client

→ Notwendige Einträge in USBSecure.ini: SmtpServer, MailFrom, MailTo1
Beim Einstecken eines unerlaubten USB-Massenspeichers sendet der Client über Ihren Mailserver eine Mail an die in der USBSecure.ini eingetragenen Mailadressen (MailTo1, MailTo2 und MailTo3). Die Kommunikation erfolgt über Port 25 (SMTP). Eine Authentifizierung findet nicht statt, den Clients muss also internes Relaying erlaubt sein.
Bitte beachten Sie, dass in einigen Umgebungen dieser Mailversand verhindert werden könnte, da das Relaying untersagt ist oder Virenscanner/Firewalls den Zugriff der Clients zum Mailserver auf Port 25 unterbinden.

Zentraler Mailversand

→ Notwendige Einträge in USBSecure.ini: UsbStorNotify=yes

Beim Einstecken eines unerlaubten USB-Massenspeichers erzeugt der Client eine Textdatei im Verzeichnis devicesRW$\Notify. Diese Dateien können in regelmäßigen Intervallen von einem Skript abgearbeitet werden, um die USBSecure-Administratoren zu benachrichtigen.
Erstellen Sie dazu einen geplanten Task „USBSecure Mail“ in der Computerverwaltung eines beliebigen Windows-Servers, der minütlich läuft und folgenden Befehl ausführt:

Aktion: Programm starten
Programm/Skript: C:\USBSecure\SmtpSend.exe
Argumente hinzufügen: <Mailserver-Name> <Abenderadresse> <Empfängeradresse> "Unbekannter USB-Massenspeicher (%COMPUTER%)" -folder:"\\<USBSecure-Servername>\devicesRW$\Notify"

Kopieren Sie die Datei SmtpSend.exe dazu in ein neu erstelltes Verzeichnis C:\USBSecure auf dem Server.

Sobald ein unzulässiger USB-Massenspeicher auf einem Client eingesteckt wird, wird im Verzeichnis **\\<USBSecure-Servername>\devicesRW$\Notify** eine Textdatei erzeugt, die dann vom geplanten Task als Mail versendet wird. Danach wird die Datei ins Unterverzeichnis „done“ verschoben.

Logdatei USBSecure.log

In der Lodatei USBSecure.log werden alle Aktionen protokolliert. Dazu gehören Benutzeranmeldungen, Start des USBSecure-Dienstes, Ein-/Ausschaltung von Geräten, Lizenznachrichten und weitere Aktionen. Der Protokollierungsgrad (Loglevel) sollte im Produktivbetrieb immer auf „normal“ stehen. Zu Diagnosezwecken kann er auf „full“ gestellt werden. Dann werden wesentlich mehr Informationen in die Logdatei geschrieben (s. Abschnitt USBSecure.ini).

Benutzer <LoggedOff>

Der Benutzer <LoggedOff> erscheint im Logfile USBSecure.log, wenn kein Benutzer angemeldet ist. Er kann nur auf Geräte zugreifen, die im [AllUsers]-Bereich aufgeführt sind. Im Standard werden bei der Windows-Abmeldung (und vor der Anmeldung) alle nicht im AllUsers-Bereich aufgelisteten USB-Geräte deaktiviert. Ist dieses Verhalten nicht erwünscht (beispielsweise weil ein USB WLAN-Adapter bereits zur Anmeldung benötigt wird), kann der Eintrag „UsbLoggedOffDeactivation=no“ in der Datei USBSecure.ini vorgenommen werden.

Schnelle Benutzerumschaltung

Mit Windows Vista wurde die schnelle Benutzerumschaltung (Fast User Switching) auch für Domänenbenutzer eingeführt. Das bedeutet, dass sich mehrere Benutzer gleichzeitig an einem Windows-PC anmelden können.
Sobald USBSecure erkennt, dass sich mehrere Benutzer angemeldet haben, schaltet es in den „FastUserSwitching“-Modus. Dadurch werden die Benutzer bezogen freigeschalteten Geräte deaktiviert. Lediglich die im AllUsers-Bereich freigegebenen Geräte bleiben freigeschaltet.