Lugrain USBSecure® 5.0

Port Security for Windows 7, Windows 8, Windows 10 and Windows 11

Installation and Configuration Guide

Lugrain USBSecure 5.0

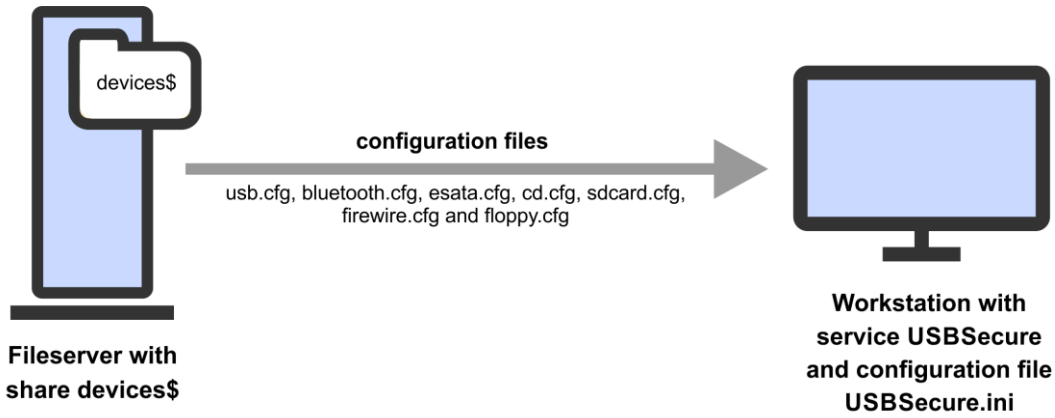
Installation Guide

Content

Functionality

Lugrain USBSecure is security software for securing the USB interfaces of client computers. USBSecure allows you to define which user can access which USB device on a per-user basis or per-computer basis. Additionally USBSecure enables or disables Bluetooth devices, CD/DVD drives, floppy drives, FireWire ports, eSATA ports and SD card readers.

USBSecure runs as a service on Windows 7, Windows 8, Windows 10 and Windows 11 (32 or 64 bit in each case). You can define the access to the devices in whitelists. When a user logs on, USB devices, Bluetooth devices, CD/DVD drives, floppy drives, FireWire ports, eSATA ports and SD card readers will be enabled or disabled on the basis of the whitelists. An existing file server or any Windows server can act as a USBSecure server, only two network shares are required. Additionally to the USBSecure service a scheduled task is installed during setup. This task starts a process USBSecureControl.exe to monitor the USBSecure service.



Required additional tools

USBSecure 3, 4 and 5 do not require any additional tools in contrast to version 1 and 2. All required files are included in the MSI package.

Installation

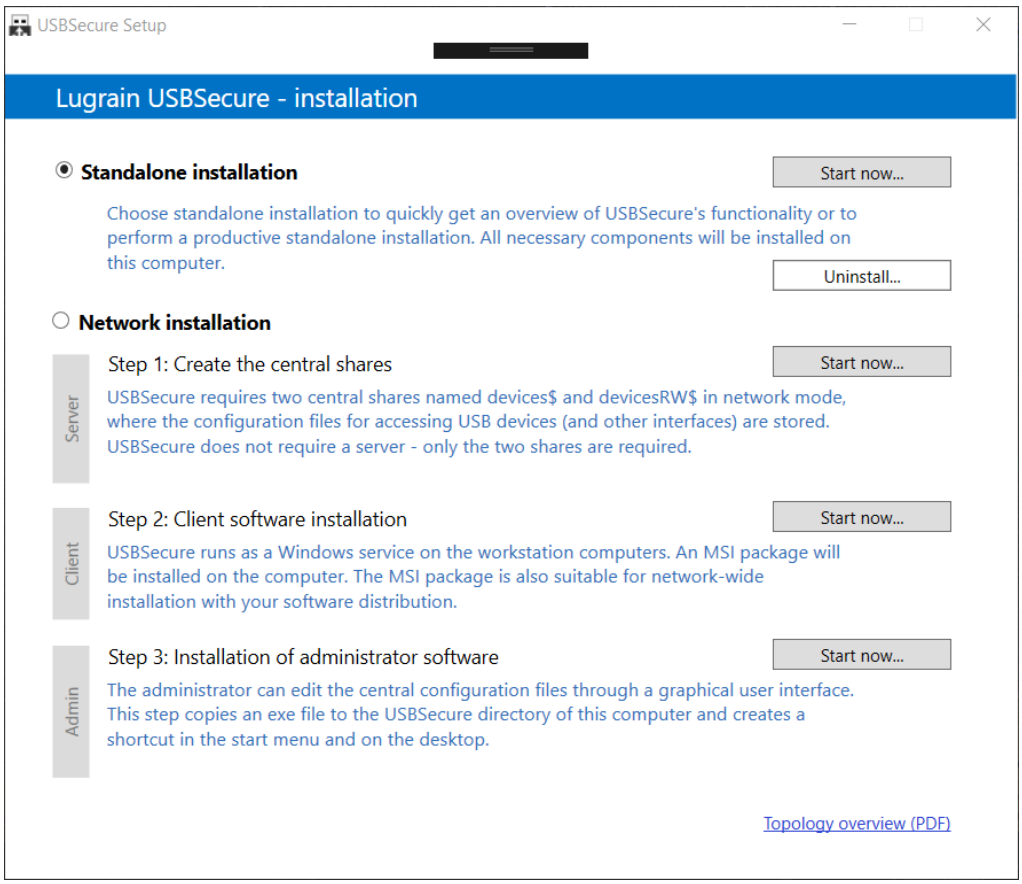
System requirements

Client: The USBSecure service (blocking / allowing devices and ports) runs without any .NET Framework software. For proper user interaction .NET-Framework 3.5 is necessary. Note: Since Windows 7 .NET-Framework 3.5 is installed by default.

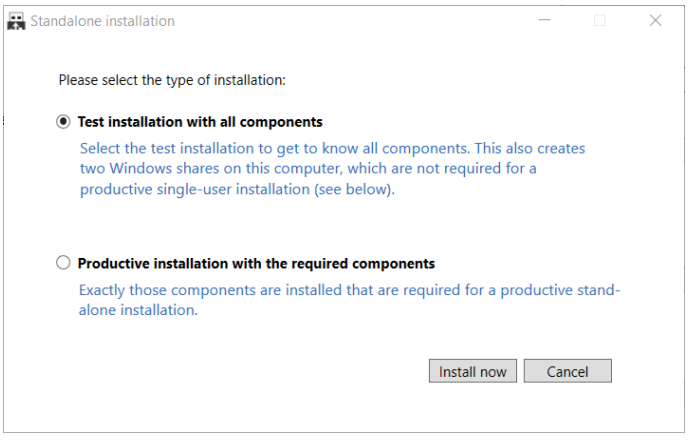
Server: Since the server consists of only two Windows shares, any Windows server (or client) can be used here without restriction. The use of a filer or NAS device is also possible.

First installation

Start the installation via the Setup.exe file and then select "Standalone installation".

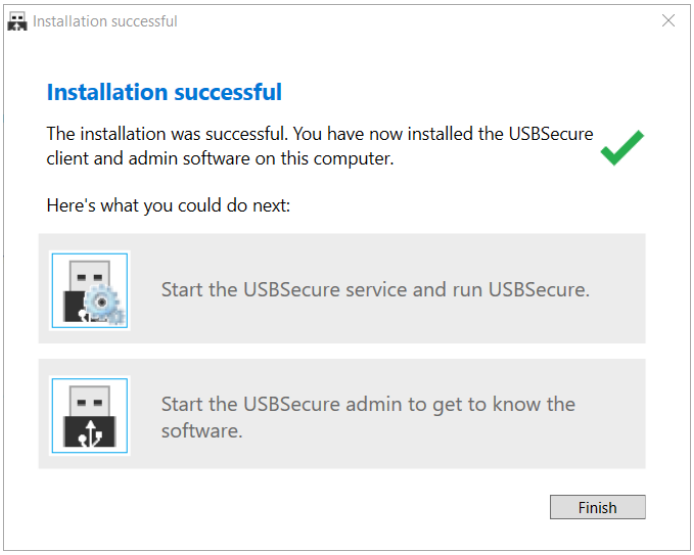


You have the option to perform a test installation to get to know USBSecure. This installs all components of a productive network installation on a single computer. These can be easily removed again with the "Uninstall" button.



After the installation is complete, you can start the USBSecure service.

Attention: With the start of the service, it is possible that certain devices of your computer will be disabled. This could include a fingerprint scanner, which is required for your login. In any case, make sure you know your login credentials before starting the service!



Testing the installation

You can now test USBSecure by making sure that USB mass storage devices (stick, hard disk, ...) are no longer allowed. In the second step we then make sure that only a very specific USB stick is allowed.

The supplied configuration file usb.cfg has the following entries so far:

```
[AllUsers]
service = usbhub   # all USB root hubs allowed
service = usbhub3  # all USB root hubs V3 allowed
service = iusb3hub # all USB root hubs V3 allowed
service = hidusb   # all USB keyboards and mice allowed
service = usbstor  # all USB mass storage devices allowed
service = usbccgp  # required for wireless keyboards and mice
service = bthusb   # USB Bluetooth Adapter
```

The entry **`service=usbstor`** in the AllUsers section allows all USB mass storage devices for all users.

Now do the following:

1. Remove the **`service=usbstor`** entry and save the configuration.
2. Apply the new configuration to your computer. To do this, enter your PC name in the dropdown field at the top right and click the down arrow (Apply to computer). Alternatively, you can also restart the "USBSecure" service (via Services).
3. Now connect a USB mass storage device to the computer, e.g. a USB stick. Since according to usb.cfg USB mass storage devices are not allowed (except for user Administrator), the USB stick will be disabled (see Device Manager, Windows Explorer or USBSecure.log).

Allow a specific USB stick

To allow a specific USB stick, proceed as follows:

1. Start the Windows Device Manager (devmgmt.msc) and identify the connected USB stick. In most cases it can be found as "USB Mass Storage Device" under "USB Controller".
2. Open the properties of the USB Mass Storage Device (right mouse button) → Details → Device Instance Path. Copy the device instance path and paste it in the AllUsers section under the service entries. The AllUsers section now looks something like this:

```
[AllUsers]
service = usbhub   # all USB root hubs allowed
service = usbhub3  # all USB root hubs V3 allowed
service = iusb3hub # all USB root hubs V3 allowed
service = hidusb   # all USB keyboards and mice allowed
service = usbccgp  # required for wireless keyboards and mice
service = bthusb   # USB Bluetooth Adapter
USB\VID_090C&PID_1000\AA201106043279   # USB-Stick
```

3. Save the configuration and apply it to your computer again or restart the "USBSecure" service.
4. The connected USB stick is now switched on and is available in Windows Explorer. If you connect a second USB stick, it will be deactivated.

You can now create additional users (+) to enable USB devices not for all but only for specific users.

Information for Windows 7/8/10/11: You may need to start USBSecure Admin with “Run as Administrator” to edit the usb.cfg file – even if you are already logged in as Administrator.

Read the "Configuration" section for details on how to allow access to individual devices and how to set up the configuration per user.

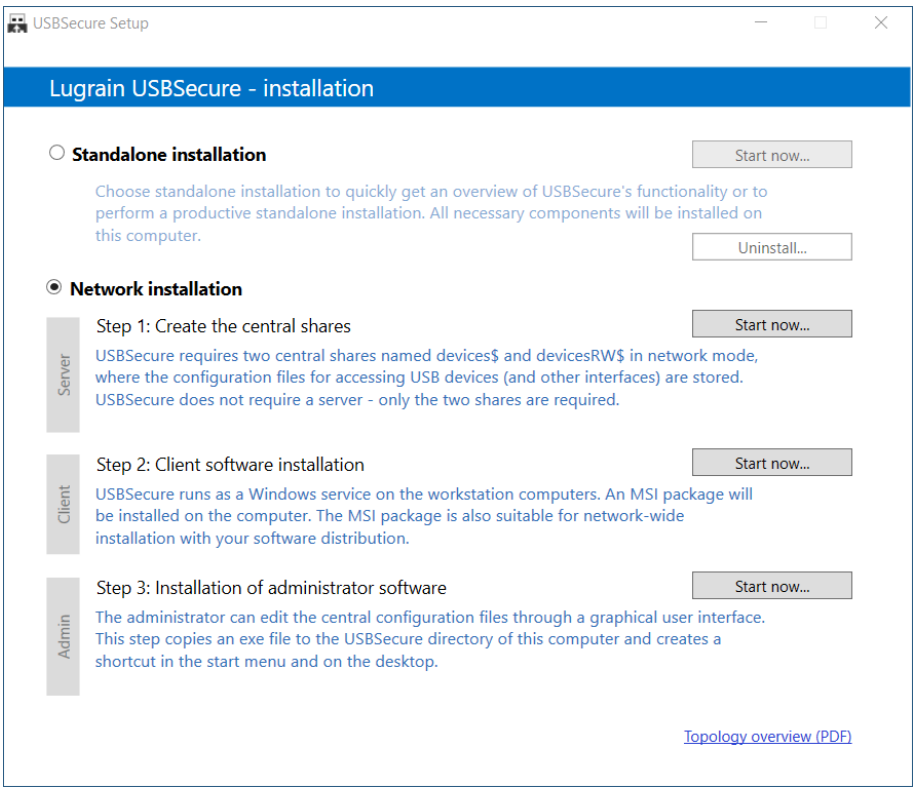
Notice: The built-in group "Users" must not have write access to the files in USBSecure folder in a productive environment → s. Chapter "Security - Hardening of the system”

Network installation

In a corporate environment, you install a central USBSecure server that provides the configuration files for the clients. As a "server" you only need two network shares.

Step 1: Run the Setup.exe file on a Windows server that will serve as the USBSecure server and select “Network Installation”. Click Step 1 → Start now → Create shares now.

Alternatively, you can create the two shares manually - for example, if you do not want to use a Windows server as the USBSecure server, but a NAS device, Linux server, or similar. To do this, click "Start now" on any computer and then "Create shares manually". The procedure is explained there in detail.



Step 2: Install the client software (MSI package) on one or more computers in your organization. The MSI configuration options are described in section "Silent installation (MSI)". For "server name", enter the name of the server on which you performed step 1. You can also change the server name later in the USBSecure.ini file.

Notice: The USBSecure server and client must be within the same Windows domain.

Step 3: Install the Admin Client on one or more computers in your organization. The Admin Client is required only by the USBSecure administrators.

If access to the server does not work

If the access to the USBSecure server doesn't work correctly (central usb.cfg is not copied to client when restarting USBSecure service), please make sure that

- Server and client are members oft the same Windows domain
- Group **Everyone** has read access to the devices$ share. "Domain Users" is not sufficient here.
- Group **Everyone** has read access to the devices$ folder. "Domain Users" is not sufficient here.

Use the following command (from a command prompt) to verify that access works for the currently logged-in user:

copy \\server-name\devices$\usb.cfg
(replace "**server-name**" by the name of your USBSecure server)

If the copy operation works, the next step is to make sure that the USBSecure service is also able to perform the copy operation. The USBSecure service performs the copy operation with system privileges. To do this, perform the following test.

For Windows Windows 7 / Windows 8 / Windows 10 / Windows 11

Download the Sysinternals PS Tools (http://www.microsoft.com/sysinternals) and run the following command from a command prompt (run as administrator):

psexec -i -s cmd.exe

Enter the copy command in the newly-opened command prompt:

copy \\server-name\devices$\usb.cfg
(replace „**server-name**" by the name of your USBSecure server)

If this copy operation succeeds the USBSecure service will also be able to copy it.

If the copy operation does not work and your devices$ share is on a storage system, first try using a "real" Windows server as the USBSecure server. The storage system may not be exactly Windows compliant.

If you don't succeed with a real Windows server, please contact support@lugrain-software.com.

Service USBSecure

The USBSecure service can‘t be stopped by **Users** or **Power Users**. Only **Administrators** are able to stop and start the service. It is also possible to prevent administrators from stopping the service (see MSI values).

Uninstall

Uninstall can be performed in Control Panel / Add/Remove Software.

Note: Please note that USB devices that have been disabled by the USBSecure service will not be re-enabled when the software is uninstalled. Enable all devices before uninstall with

[AllUsers]
*

and restart the USBSecure service or activate the devices later in Device Manager.

Silent installation (MSI)

You can implement USBSecure installation without any user interaction with the following command:

msiexec /i USBSecure.msi /qb USBSECURE_SERVERNAME=<Name of USBSecure server> INSTALLDIR="C:\Program Files\USBSecure" LICENSEKEY=AAAAA-BBBBB-CCCCC-DDDDD-EEEEE

Provide your license key behind the keyword **LICENSEKEY=**. You can find the license key for the free 5-PC version as a text file included in the download.

Other values that can be set during automatic installation:

INIOVERWRITE=<time in minutes>
This value specifies when the local configuration file USBSecure.ini will be overwritten by a centralized version. The centralized USBSecure.ini must be located in the devices$ share. SBSecure.ini überschrieben wird. **<time in minutes> defines the time since the USBService start.** If you specify this MSI value it will overwrite the entry in USBSecure.ini. Example: INIOVERWRITE=15

NOUSBSTORINFO=<yes|no|warn>
Defines the behavior when inserting a forbidden USB mass storage device (see USBSecure.ini). If you specify this MSI value it will overwrite the entry in USBSecure.ini. Example: NOUSBSTORINFO=no

ADMINSCANTSTOP=<0|1>
Specifies wether the USBSecure service can be stopped / restarted by administrators or not. Value ADMINSCANTSTOP=1 prevents administrators to stop and restart the service. If you specify this MSI value it will overwrite the entry in USBSecure.ini. Example: ADMINSCANTSTOP=0

NETWORKADMINSCANSTOP=<0|1>
Only in combination with ADMINSCANTSTOP. Specifies wether the USBSecure service can be stopped / restarted by administrators over the network or not. Please note that it’s “CAN” in this case. NETWORKADMINSCANSTOP =1 allows administrators to stop and restart the USBSecure service when connected over the network, e.g. via computer management. This MSI value will NOT be inserted in USBSecure.ini. Example: NETWORKADMINSCANSTOP =1

MINKEYBOARDCOUNT=<count>
Sets the maximum number of keyboards allowed at the same time to the value <count>. This is the value that will later be in the KeyboardCount.cfg file. Addresses the problem that PCs often do not

have a keyboard connected during the operating system installation. The KeyboardCount.cfg file then contains a 0. Set MINKEYBOARDCOUNT=1 so that there is at least a 1.

USB_CONFIGFILE=<filename>
Allows to specify a pre-configured USB configuration file (usb.cfg) already during installation. The file can be specified without a path if it is located in the same folder as the USBSecure.msi file. Example 1: USB_CONFIGFILE=usb.cfg. Example 2: USB_CONFIGFILE=”X:\MyFiles\usb.cfg”, Example 3 (in subfolder): USB_CONFIGFILE=“.\MyFiles\usb.cfg“.

INIFILE=<filename>
Allows to specify a pre-configured USBSecure configuration file (USBSecure.ini) already during installation. The file can be specified without a path if it is located in the same folder as the USBSecure.msi file. Example 1: INIFILE=USBSecure.ini. Example 2: INIFILE ="X:\MyFiles\USBSecure.ini", Example 3 (in subfolder): INIFILE=“.\MyFiles\USBSecure.ini“.

CONFIGFILES=<filepattern> (only OT-Version)
Allows all .cfg files to be included during installation. Can be specified without a path if the files are in the same folder as the USBSecure.msi file. Example 1: CONFIGFILES=*.cfg. Example 2: CONFIGFILES ="X:\MyFiles*.cfg".

DEVICELOGGING=yes|no (only OT version)
Specifies whether a local logging of all plugged in and unplugged devices is to take place in the DeviceLogging.log file.

The command for silent uninstall:

msiexec /x USBSecure.msi /qb

Upgrade from an older version

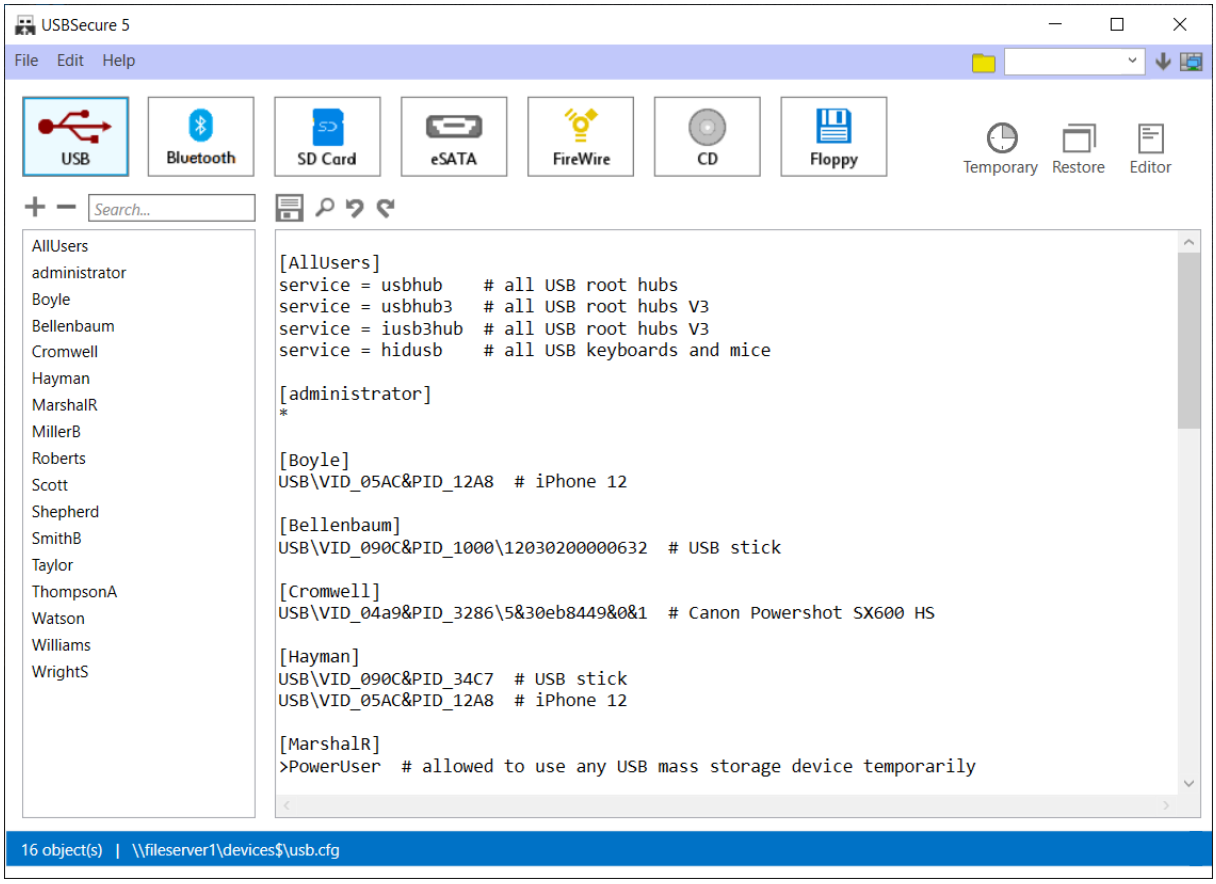
The upgrade from an older USBSecure version always consists of an uninstall and reinstall. Configuration settings are not lost in a network installation because they are stored centrally in the devices$ share. In a local installation (stand-alone) please backup all .cfg files and the USBSecure.ini file and copy them into the folder after reinstall.

If you are upgrading from an older version than version 4.4 to version 5, proceed as follows:

1. Copy the bluetooth.cfg file from the "Server" directory of the installation media to your existing devices$ share.
2. Replace the administration GUI USBSecure-Admin.exe with the new version from the "Admin" directory on the installation media.
3. Reinstall the USBSecure.msi client software from the "Client" directory of the installation media.

Configuration

Configuration files (.cfg files) can be configured with a graphical user interface. The GUI requires .NET Framework 4.5 on your computer. A direct configuration of the files via editor is still possible, but not recommended.



Configuration files

The configuration files ***usb.cfg, bluetooth.cfg, sdcard.cfg, esata.cfg, firewire.cfg, cd.cfg*** *and* ***floppy.cfg*** are whitelists containing allowed devices. Users not listed in these files do not have access to the devices.
The [AllUsers] section in ***usb.cfg*** and ***bluetooth.cfg*** and the AllUsers entry in floppy.cfg, cd.cfg, esata.cfg, sdcard.cfg and firewire.cfg are valid for all users. The .cfg files are maintained centrally in the devices$ share. They are copied to the client's USBSecure folder whenever the service starts. The USBSecure service always accesses the locally stored files.

USBSecure.ini is a static file in the client's USBSecure folder. It contains global settings (name of the USBSecure server, loglevel etc.).

New from USBSecure version 3: Parameter **IniOverwrite** for centralized management of the USBSecure.ini file (see below).

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

Users who should have access to floppy drives, CD/DVD drives, FireWire ports, eSATA devices or SD cards, must be listed in the files ***floppy.cfg, cd.cfg, esata.cfg, sdcard.cfg*** and ***firewire.cfg*** (one user per line):

```
UserA
UserB
UserC
```

If you would like to configure all users to have access, you can make the following entry „AllUsers“ in the appropriate file:

```
AllUsers
```

Unlike USB devices, access to individual, specific devices cannot be configured for floppy drives, CD/DVD drives, Firewire interfaces, eSATA interfaces and SD cards. Once a user is entered in the corresponding .cfg file, access to all devices of the type is allowed.

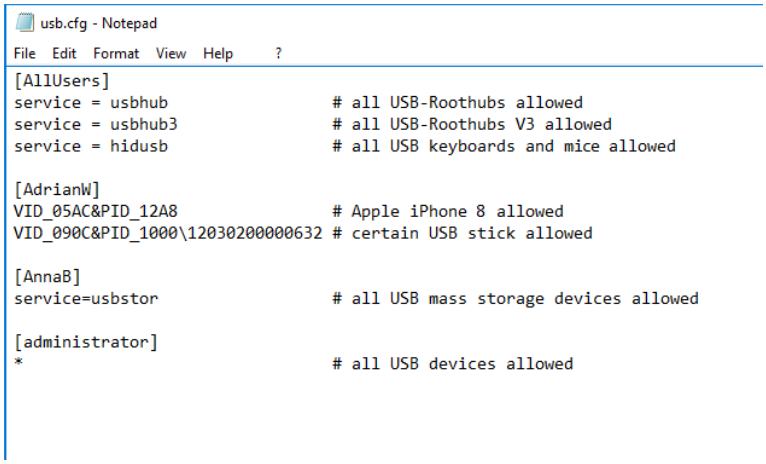
usb.cfg

File usb.cfg manages the user's access to USB devices. User names must be written in brackets **[ ]**. Below the user name the allowed USB devices are listed. File usb.cfg contains an AllUsers section and a per-user section:

```
[AllUsers]
…

[UserA]
…

[UserB]
…

[UserC]
…
```

The names of the USB devices are taken from the Device Manager. You can obtain the device identifiers (VID/PID) by launching the script ***ShowExistingUsbDevices.vbs***. The script generates the file ***ExistingUsbDevices.txt***, in which all USB devices installed on the computer are listed in the desired notation. You can paste them directly into your central usb.cfg file.

Alternatively you can retrieve the VID/PID identifiers from the USBSecure logfile (USBSecure.log) or from Windows Device Manager.



Text behind the hash sign (#) is a comment and will be ignored.

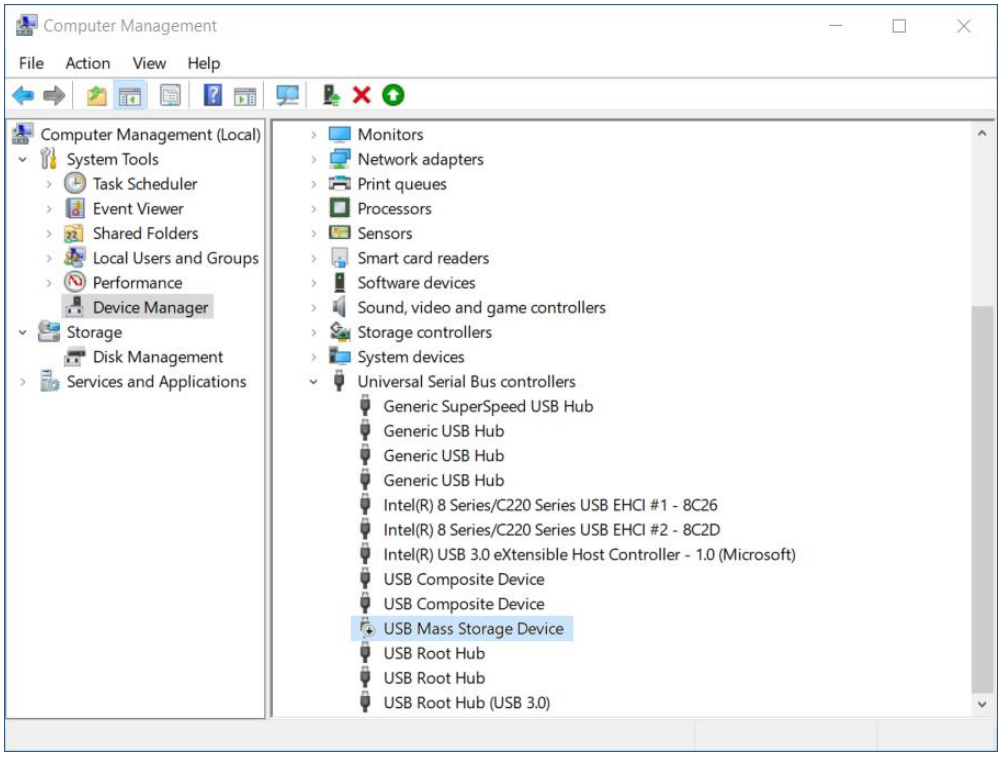
Privileged users with access to all USB devices get an asterisk (*):

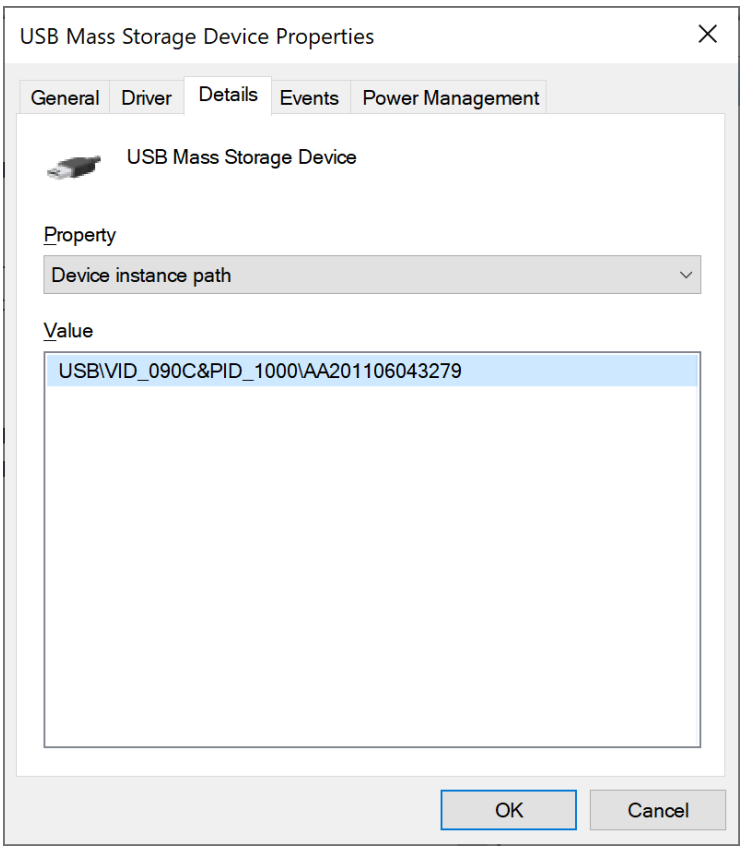
```
[UserA]
*
```

The [AllUsers] section lists devices that are enabled for all users. You should at least have the line „service = usbhub“ and „service = usbhub3“ in this section. Normally „harmless“ devices like keyboards, mice and scanners are listed here.

The configuration of a user always results from the sum of the AllUsers configuration and the personal configuration. For example, if all USB root hubs and all USB mice and keyboards are enabled in the AllUsers section and all USB mass storage devices are enabled in the user's personal section, then all USB root hubs, all USB mice and keyboards and all USB mass storage devices are enabled for the user.

You can right-click the USB device in Windows Device Manager to retrieve the identifier. In this case you would insert **VID_090C&PID_1000\AA201106043279** into usb.cfg to allow exactly this certain USB mass storage device:





It is also allowed to use the term **USB\VID_090C&PID_1000\AA201106043279** with prefix **\USB**, so you can copy the ID directly from Device Manager.

If you would like to allow any USB mass storage device of the same model or type, you can specify VID_090C&PID_1000 (or USB\VID_090C&PID_1000).

Wildcard question mark

Use the question mark "?" to place a wildcard for a character:

```
VID_1234&PID_????
```

This makes it possible to allow all devices from a specific manufacturer: You enter the VID (Vendor ID) and leave the PID (Product ID) variable. For example, to allow all devices from the manufacturer Kyocera, you could use the following expression: VID_0482&PID_????

Case sensitivity

The case is not relevant in all USBSecure configuration files. Entry VID_090C&PID_1000 and entry Vid_090C&Pid_1000 are considered identical.

Allow USB devices per computer

From version 4.4 it is possible to allow USB devices "per computer". This is useful if a specific USB device is connected to a specific computer to which several users log on. Use the following notation for this:

```
[Host:<computername>]
<allowed device>
```

Example:

```
[Host:PC1234]
VID_090C&PID_1000
```

The entries add up if there are applicable entries for both the user and the computer the user logs on to.

Services

To enable entire devices classes please use the „service“ command: service=<Service-Name>

Example: `service = usbstor`

Often used values:

service=usbhub	USB root hubs
service=usbhub3	USB3 root hubs
service=iusb3hub	USB3 root hubs
service=hidusb	USB keyboards and mice
service=usbstor	USB mass storage devices (sticks, hard disks…)
service=uaspstor	USB SCSI hard disks
service=usbprint	USB printers
service=usbscan	USB scanners
service=usbvideo	USB cameras

You can determine the service of a USB device in Device manager / Properties of the device / Service.

Devices allowed by default

From USBSecure version 4.3 certain USB devices are enabled by default – they do not have to be listed in the usb.cfg file. These are devices with one of the following values in the „service“ field: usbhub, usbhub3, iusb3hub or hidusb. This feature avoids total loss of functionality in cases of misconfiguration. If you would like to disable these services anyway, please use the following notation in the AllUsers section:

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

Example: `no-defaultservice = hidusb`

Users

Users can be specified in the following notation:

[user] Only the user is listed. The domain is arbitrary. The settings are valid for local and domain users.
Example: [RalphG]

[domain\user] Domain and user
Example: [lugrain\RalphG]

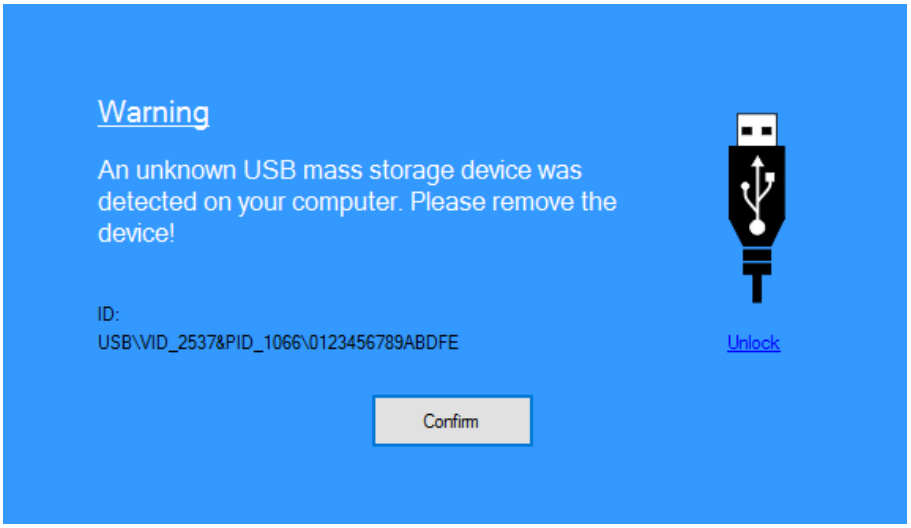
[user@domain] User and domain
Example: [RalphG@lugrain]

Power Users

PowerUsers are allowed to use all USB mass storage devices (sticks, USB disk drives) temporarily. If a PowerUser inserts a forbidden USB mass storage device, an additional link “Unlock” will be displayed in the blue notification window. This allows the user to enable the mass storage device until the next USBSecure service startup.

Please use the following syntax:

```
[username]
>PowerUser
```



Static Devices

You can make static entries for particularly important USB devices. Static entries are characterised by the fact that they cannot be deleted again centrally with the Admin GUI. This prevents misconfigurations in the Admin GUI from causing a specific USB device to no longer function.

Use the keyword "static:" to make a static entry:

```
static:<USB device>
```

Example:

```
[Host:PC1234]
static:usb\vid_1234&pid_5678
```

When a client encounters a static entry, it creates (30 sec. after service start) a file *StaticUsbDevices---<hostname>.cfg*, which is not deleted again. This file contains the USB device - in the example usb\vid_1234&pid_5678. The USB device is thus always allowed on this client, regardless of the user.

In order to delete a static device entry, the file on the client must also be deleted in addition to the removal in the admin interface. The file is located directly in the USBSecure directory, usually C:\Program Files (x86)\USBSecure.

Static entries are not allowed in the AllUsers area. They are ignored there. More precisely: They are regarded as normal entries (without static).

Recommendation for the use of static devices:

- Use static entries **sparingly**! Intensive use contradicts central administration.
- Use static entries preferably for computers → [Host:PC1234] and less for users. A user who has a static entry takes it with him to every computer he logs on to. There, in turn, the USB device is allowed for all users.

If a file *StaticUsbDevices---<hostname>.cfg* already exists on a computer, it will be expanded if an additional static entry is found.

ignore entries

Use the prefix “ignore:” to ensure that no blue notification window, no locking of the computer and no mail notification occurs for certain USB mass storage devices. This mechanism is useful when, for example, built-in card readers appear as a new device in certain situations and cause a notice unnecessarily. This can happen, for example, when connecting a switched-on notebook to the docking station.

```
ignore:<USB device>
```

Example:

```
[Host:PC1234]
ignore:usb\vid_1234&pid_5678
```

The USB device usb\vid_1234&pid_5678 is thus still not allowed, but no notification appears when you plug it in.

Blacklist services

From USBSecure Version 3.3 you can work with blacklists in usb.cfg. This allows configurations like *"Allow all users any USB device except USB mass storage devices"*. Blacklist services can be applied in the following notation:

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

Example: `blacklist-service = usbstor`

Note: Whitelists override blacklists! If a user has the entries **blacklist-service = usbstor** and **service = usbstor**, USB mass storage devices will be allowed.

Example configurations usb.cfg

You would like to...

...allow only USB keyboards and mice, nothing else:

```
[AllUsers]
service = usbhub    # USB root hubs should always be allowed
service = usbhub3   # USB root hubs should always be allowed
service = hidusb    # any USB keyboard and mouse allowed
```

... allow only USB keyboards and mice, nothing else. Allow a certain USB stick for user miller:

```
[AllUsers]
service = usbhub    # USB root hubs should always be allowed
service = usbhub3   # USB root hubs should always be allowed
service = hidusb    # any USB keyboard and mouse allowed

[miller]
VID_090C&PID_34C7   # VidPid of the stick, see device manager
```

... allow only USB keyboards and mice, nothing else. But allow additionally USB mass storage devices for user smith:

```
[AllUsers]
service = usbhub    # USB root hubs should always be allowed
service = usbhub3   # USB root hubs should always be allowed
service = hidusb    # any USB keyboard and mouse allowed

[smith]
service = usbstor   # USB mass storage devices
service = UASPStor  # USB mass storage devices (newer)
```

... allow only USB keyboards and mice, nothing else. But allow additionally any USB device for user Administrator:

```
[AllUsers]
service = usbhub    # USB root hubs should always be allowed
service = usbhub3   # USB root hubs should always be allowed
service = hidusb    # any USB keyboard and mouse allowed

[administrator]
*
```

...allow any USB device for everyone, but no USB mass storage devices:

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

... allow any USB device for everyone, but no USB mass storage devices. But allow additionally any USB mass storage device for user Administrator and a certain USB mass storage device for User Smith:

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


[administrator]
service = usbstor   # USB mass storage devices
service = UASPStor  # USB mass storage devices (newer)


[Smith]
VID_090C&PID_34C7   # VidPid of the stick, see device manager
```

bluetooth.cfg

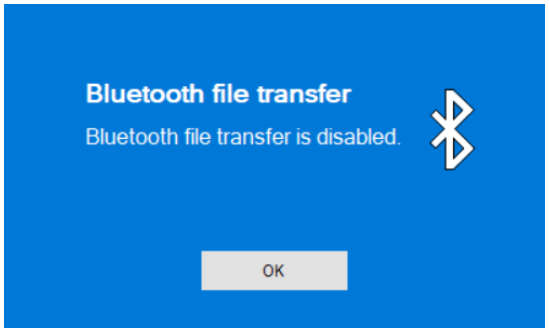
Access to Bluetooth devices is specified in the bluetooth.cfg file. As in the usb.cfg file, there is a AllUsers section and a section per user:

```
[AllUsers]
…

[UserA]
…

[UserB]
…
```

As in the usb.cfg file, it is possible to allow Bluetooth devices per user and per computer. Services can also be allowed. However, there are no blacklist services and no power users, but there are the entries AllowFileTransfer and AllowPanNetwork.

AllowFiletransfer

Use AllowFiletransfer=no to prevent the transfer of files and folders via Bluetooth. A file can be transferred via Bluetooth between two paired devices by right-clicking on the file → Send to → Bluetooth device. AllowFiletransfer=no checks periodically (every 8 seconds) whether the graphical user interface for Bluetooth file transfer is started. If so, it is terminated and a blue message window is displayed.



Please note: AllowFiletransfer=yes "beats" AllowFiletransfer=no. This makes it possible to globally prevent file transfer (AllowFiletransfer=no in the AllUsers section) and to allow it only for individual users (AllowFiletransfer=yes in the user section).

AllowPanNetwork

Use AllowPanNetwork=no to prevent participation in a PAN (Personal Area Network) network via Bluetooth. A PAN network is a wireless network via the Bluetooth interface. It can be easily set up by clicking on the Bluetooth icon in the system tray → "Join a Personal Area Network". AllowPanNetwork=no deactivates the virtual network card "Bluetooth device (Personal Area Network)", which means that it is no longer possible to create a PAN network.

Please note: AllowPanNetwork=yes "beats" AllowPanNetwork=no. This makes it possible to globally prevent the creation of PAN networks (AllowPanNetwork=no in the AllUsers section) and to allow it only for individual users (AllowPanNetwork=yes in the user section).

All Bluetooth settings only take effect when there is a functional Bluetooth interface. The Bluetooth interface itself is usually a USB device and must therefore be activated in the usb.cfg file.

Bluetooth configuration example 1: Allow all Bluetooth devices, don't allow file transfer

One piece of information in advance: The activation of Bluetooth devices is more complicated than the activation of USB devices. While with USB devices in most cases there is exactly one entry in Device Manager for a device, with Bluetooth it is usually necessary to activate several virtual devices in order to be able to use a real device.
For this reason, this configuration example is very interesting. It prohibits file transfer via Bluetooth - with the least administrative effort.

The aim in this example is to globally allow all Bluetooth devices, but to prevent file transfer via Bluetooth.

First make sure that your Bluetooth interface works. In many cases, a USB device must be activated for this - the actual Bluetooth interface. For example, the device could be named "Intel® Wireless BlueTooth®" or "Broadcom Bluetooth Adapter".

The AllUsers area of the bluetooth.cfg file looks as follows by default:

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

► Step 1: Change the entry that allows file transfer of files and folders:

```
AllowFiletransfer=no
```

This entry prevents the file transfer by *clicking the right mouse button → Send to → Bluetooth device* and by *clicking on the Bluetooth icon in the system tray → Send a File*.

► Step 2: Change the entry that allows the creation of PAN networks:

```
AllowPanNetwork=no
```

This entry prevents setup and participation in a PAN (Personal Area Network) via Bluetooth.

We get the following AllUsers area:

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

With this configuration, the virtual Bluetooth GUI is disabled and the virtual network card "Bluetooth device (Personal Area Network)" are deactivated. The goal is achieved to allow all Bluetooth devices, but to prevent file transfer via Bluetooth.

If you want to enable file transfer for individual users or computers, you can use the respective entry with "yes" in the section of the user or computer ("yes" overwrites "no"):

```
[MillerM]
AllowFiletransfer=yes
```

or

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

Bluetooth configuration example 2: Allow a Bluetooth mouse

The aim in this example is to enable the Microsoft Bluetooth Mouse 3600 for all users - all other Bluetooth devices should be forbidden. The example can be transferred to any other Bluetooth mouse.

The AllUsers section of the bluetooth.cfg file looks as follows by default:

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

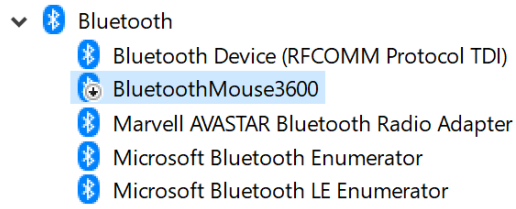
► Step 1: Remove the asterisk (*) that allows all Bluetooth devices for all users. We then receive the following AllUsers area:

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

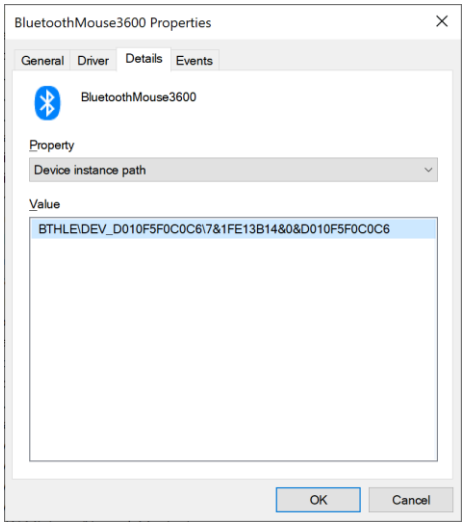
Warning: If you perform this step in your productive environment, Bluetooth devices will no longer work!

► Step 2: Connect the Bluetooth mouse via Settings Bluetooth and other devices

The Bluetooth mouse is deactivated after connecting.



► Step 3: Enter the device instance path of the "BluetoothMouse3600" device from device manager into the AllUsers section:

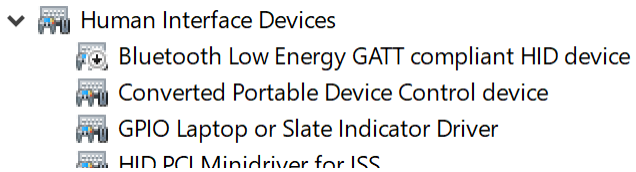


The AllUsers area now looks like this:

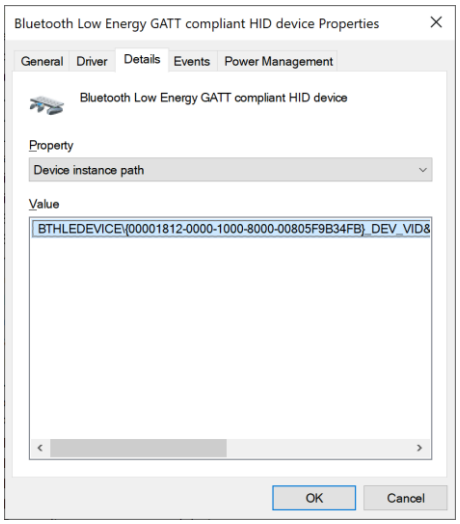
```
[AllUsers]
AllowFiletransfer=yes
AllowPanNetwork=yes
service=UmPass
BTHLE\DEV_D010F5F0C0C6\7&1FE13B14&0&D010F5F0C0C6
```

The "BluetoothMouse3600" device will be enabled after restarting the USBSecure service. However, the mouse still doesn't work.

Under "Human Interface Devices" there is another device that has to be enabled:



► Step 4: Enter the device instance path of the device "Bluetooth Low Energy GATT compliant HID device" from device manager into the AllUsers area.



Only the fixed front part of the device instance path is entered so that all devices of the same type are activated:

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

BluetoothMouse3600 will be enabled and works after restarting the USBSecure service.

► Problem: The device instance path of the BluetoothMouse3600 device is very variable. Even after removing and reconnecting the mouse, the device instance path changes:

before:

```
BTHLE\DEV_D010F5F0C0C6\7&1FE13B14&0&D010F5F0C0C6
```

after:

```
BTHLE\DEV_D011F6F0C0C6\7&1FE13B14&0&D011F5F1C0C6
```

The problem could be solved with the following entry:

```
BTHLE\DEV_D01?F6F?C0C6\7&1FE13B14&0&D01?F5F?C0C6
```

A question mark (?) stands for one character. However, only the problem for this particular mouse would be solved. Another identical mouse can have a completely different device instance path.

► Solution: Display names can be used in the bluetooth.cfg file. These are the names that can be seen in device manager. In our case, the display name is "BluetoothMouse3600". The complete bluetooth.cfg now looks like this:

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

Please note that not all display names can be used. To obtain a list of usable display names, please run the VBS file ShowBluetoothDisplaynames.vbs in the USBSecure directory.

Bluetooth configuration example 3: Allow a SmartPhone

The aim in this example is to enable a specific SmartPhone (Android or iPhone) for the AD user MillerM. The connection should be made via Bluetooth - all other Bluetooth devices should be forbidden. The configuration file bluetooth.cfg looks as follows in the standard:

```
[AllUsers]
*
service=UmPass
```

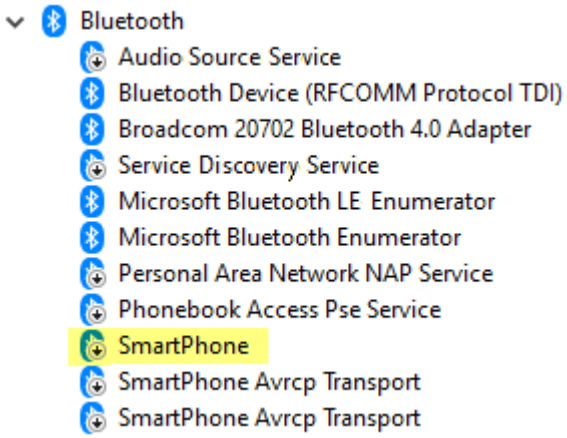
► Step 1: Remove the asterisk (*) that allows all Bluetooth devices for all users. We then receive the following AllUsers area:

```
[AllUsers]
service=UmPass
```

Warning: If you perform this step in your productive environment, Bluetooth devices will no longer work!

► Step 2: Connect the SmartPhone via Settings Bluetooth and other devices

The SmartPhone will be deactivated after connecting.

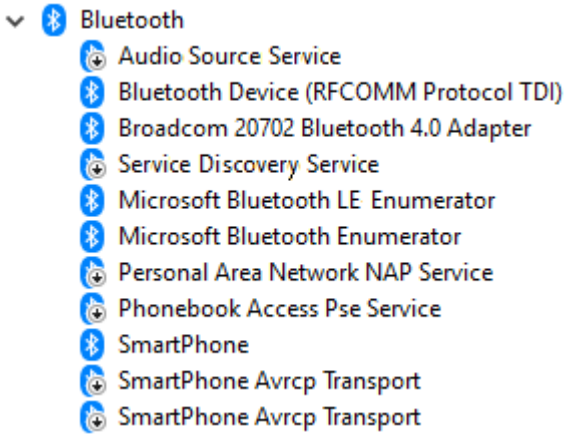


► Step 3: Enter the device instance path of the "SmartPhone" device from device manager in the section for user MillerM:

Configuration file bluetooth.cfg now looks like this:

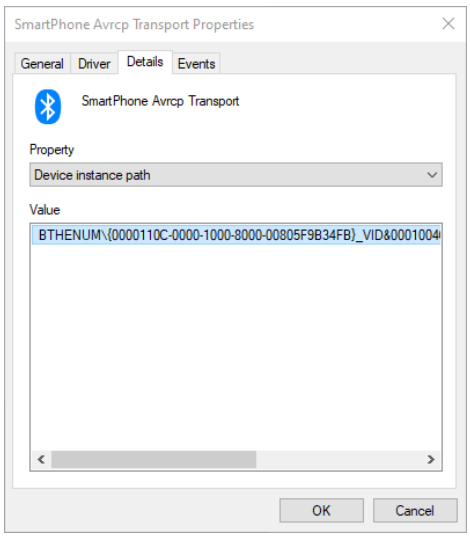
```
[AllUsers]
service=UmPass

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

The "SmartPhone" device will be enabled after restarting the USBSecure service. However, there are still some deactivated devices:



Now the device instance paths of all deactivated devices should be entered for MuellerM. But there is also an easier way:

We need the device instance path of one of the deactivated devices, for example that of the "SmartPhone AVRCP Transport" device.



When comparing the device instance paths of all devices that are still deactivated, it is noticeable that they differ only slightly from one another. We replace the deviating numbers with question marks (?):

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

► Step 4: Enter the variable device instance path for all devices that are still deactivated:

```
[AllUsers]
service=UmPass

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

The SmartPhone is enabled and works after restarting the USBSecure service.

USBSecure.ini

USBSecure.ini contains global settings. Normally you don't have to change these settings.

Server=<name of the USBSecure server>

Specify the server with the devices$ share here (see chapter „Network installation"). This value is automatically inserted during the client installation (MSI package).

LogLevel=<normal|full>

Determines the detail level of logfile USBSecure.log. In production environments this setting should be „normal". Use „full" only for problem analysis.

ViolationReboot=<yes|no>

Defines the behaviour in case of devices that couldn't be deactivated by the operating system without reboot – because they are currently accessed. ViolationReboot=yes means that a reboot is forced.

RebootDelay=60

RebootDelay defines the user's remaining time (in seconds) to save his unsaved documents in case of a ViolationReboot.

RebootMessage=Unregistered USB-, CD/DVD- or Floppy drive detected...

The message that appears in case of a ViolationReboot.

ViolationEject=<yes|no>

Determines if a removable media device (USB stick, CD, …), that couldn't be deactivated by the operating system (because it is currently accessed), should be ejected. An ejected devices must be plugged in again to function for a permitted user.

ScsiSupport=<yes|no>

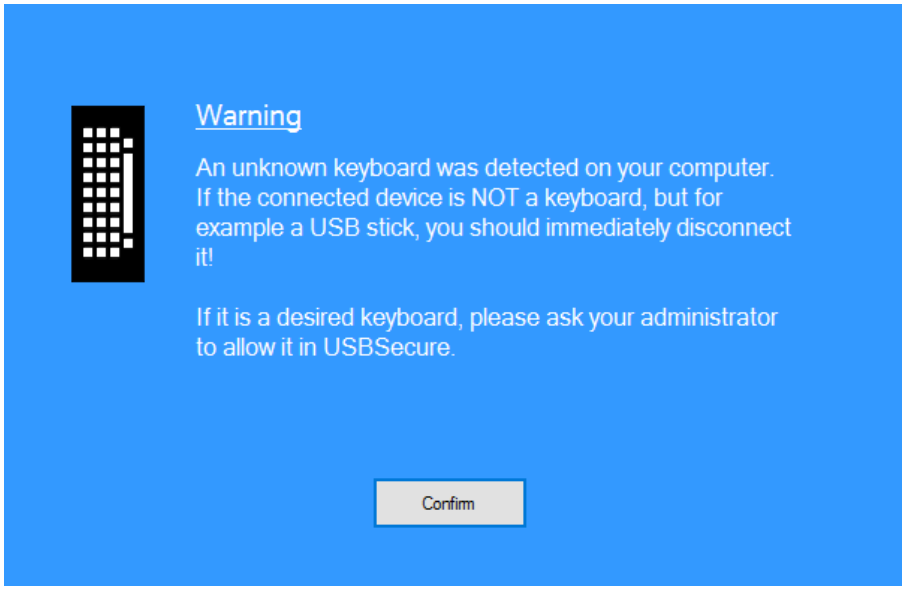
Defines if SCSI CD drives should be supported.

UsbLoggedOffDeactivation=<yes|no>

USB devices not listed in the AllUsers section will be deactivated by default, if no user is logged on. This also happens at startup and shutdown. Under some conditions this behavior is not desired, because a certain USB device is required for the logon process, e.g. a wireless device. With "UsbLoggedOffDeactivation=no" USB devices are not disabled when the user logs off, but only when a new user logs on without permissions.

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

USB devices with manipulated firmware can be used to compromise computers by emulating a keyboard (BadUSB). USBSecure detects the number of installed keyboards during its first run (if KeyboardInstall=block or KeyboardInstall=warn is configured) and writes the value into the file KeyboardCount.cfg. If a new keyboard is plugged in, the computer will be locked and the user gets a notification. In mode KeyboardInstall=warn there is just one warning. If the device is a real keyboard it can be used after confirmation by the user. In mode KeyboardInstall=block the computer will be locked permanently until the device is removed.



You can configure the number of allowed keyboards in the local file KeyboardCount.cfg (in the USBSecure folder). Increase the value or delete the file and restart the USBSecure service. Important: In USBSecure.ini KeyboardInstall=warn or KeyboardInstall=block must be configured.

LocalDevicesCopy=30

Specifies whether the text files with installed USB devices of all users should be stored centrally. Read/Write share devicesRW$ with folder ExistingUsbDevices must exist (value in minutes, 0=never).

IniOverwrite=15

Controls the central management of file USBSecure.ini. Defines whether file USBSecure.ini should be overwritten by the centrally stored USBSecure.ini (from devices$). Value in minutes, 0=never. Has no effect if the centrally stored USBSecure.ini does not exist.
It is possible to implement different languages for the USBSecure user dialogs (unknown mass storage device and new keyboard) with this setting. Depending on the operating system language, different USBSecure.ini files are copied from the central devices$ share. In the USBSecure.ini file you can define the dialog phrases (see below). Please use the following file names for the language specific USBSecure.ini files: USBSecureLanguage<InstallLanguage>.ini. The <InstallLanguage> value matches the registry value **InstallLanguage** under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language. In case of an English operating system the name would be USBSecureLanguage0409.ini.

Example: You have German, English and French clients in your company and would like to adapt the USBSecure dialogs to the respective national language. Set parameter IniOverwrite to 5 – this can also be done with MSI parameters during installation. Create the following files in the central share \\<YourServer>\devices$:
USBSecureLanguage0407.ini, USBSecureLanguage0409.ini und USBSecureLanguage040c.ini. Use the USBSecure.ini from your local installation (C:\Program Files (x86)\USBSecure) as your template. Create german dialog phrases (e.g. TextUsbWarning1, see below) in USBSecureLanguage0407.ini, english dialog phrases in USBSecureLanguage0409.ini and french dialog phrases in USBSecureLanguage040c.ini. The appropriate .ini files will be copied 5 minutes after startup of the USBSecure service (IniOverwrite=5) to the local USBSecure folder.

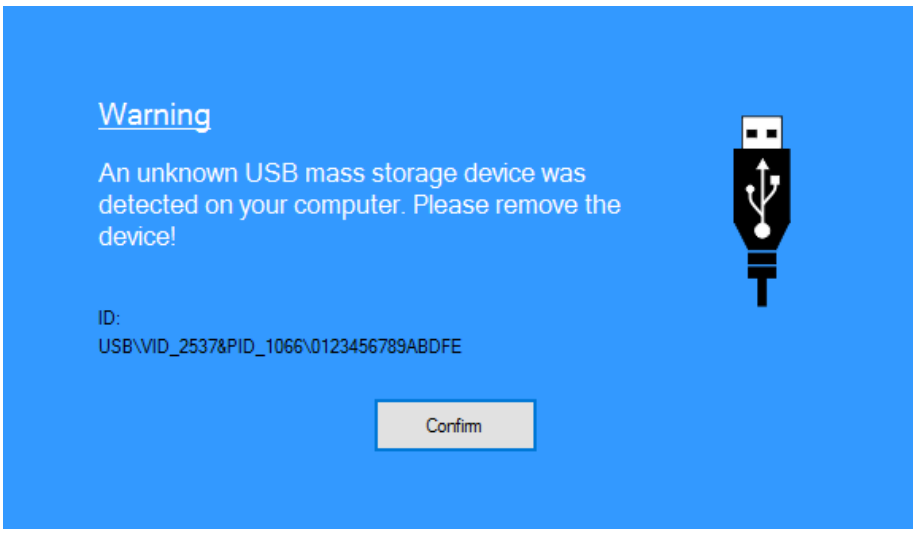
If no language specific USBSecure.ini filed exists, USBSecure.ini will be used. If the devices$ share doesn’t contain any USBSecure.ini file, nothing happens.

Backup=60

With this setting your local client machine becomes a USBSecure backup machine. All .cfg files and the USBSecure.ini from the devices$ share will be backup up to your local machine into folder **backup** every 60 minutes (value in minutes, 0=never). The files get a time stamp in the filename – old files are not overwritten.

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

When inserting a forbidden USB mass storage, a warning message will be displayed and the computer is locked. Specify NoUsbStorInfo=yes here to surpess this behaviour. USBSecure then behaves like version 3.3 – the USB mass storage device will be disabled only.
The warning message doesn’t appear when a mass storage device is already plugged at boot time.



You can set this value during unattended installation with MSI variable NOUSBSTORINFO=yes.

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

In the case of USB mass storage devices that cannot be deactivated under unfavorable conditions, ForceUsbstorUnplug=yes locks the computer again and again with a delay of about 20 seconds until the USB mass storage device has been removed.

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

With ResolveVendors=no the vendor will NOT be resolved in logfile entries.

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

If SmartphoneInfo=yes is configured, the blue warning message will also be displayed when forbidden smartphones, cameras and similar devices are connected to the computer. By default the warning message only appears by connecting USB storage devices (Service USBSTOR). In detail: If SmartphoneInfo ist set to yes, the blue warning message appears if an USB device is connected that has the value WUDFrd or WUDFWpdMtp in the Service field (see Device Manager oder DeviceTool).

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

When you set UsbStorNotify=yes, a text file will be created in the share devicesRW$\Notify when a forbidden USB mass storage device (stick, hard disk) is plugged in. This information can be used to send notification mails with the SmtpSend.exe utility (bin folder).

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

Since version 4.3, newly copied usb.cfg files are checked for plausibility. If a new usb.cfg is less than 15 bytes large, the new usb.cfg will not be used. It will also not be used if file size is less than 50% of the previous usb.cfg file. In these cases the usb.cfg file from folder “cache” will be used. This bebaviour reduces the risk of misconfiguration. If UsbCfgSizeCheck is set to „no“, no plausibility checks will be performed.

SmtpServer=<mailserver name>
MailFrom=<sender>
MailTo1=<recipient1>

MailTo2=<recipient2>
MailTo3=<recipient3>

Specify the sender, recipients and the name of your mailserver here. When a forbidden USB mass storage device (stick, hard disk) is plugged in, these recipients will be notified. Please specify at least values for SmtpServer, MailFrom and MailTo1. These settings are independent of the UsbStorNotify value.

Define your own text to be displayed when a forbidden USB mass storage device is plugged in. „\n“ for a new line:

TextUsbWarning1=Warning
TextUsbWarning2=An unknown USB mass storage device was detected on your computer. Please remove the device!
TextUsbUnlockLink=Unlock
TextUsbConfirmButton=Confirm
TextUsbUnlock1=You are allowed to enable this USB mass storage device temporarily.\n\nNote: This operation will be logged.\n\nWould you like to enable this mass storage device now?
TextUsbUnlock2=Device was enabled. It may be necessary to unplug and reconnect it.
TextUsbMsg=Your computer was locked because of an unknown USB mass storage.\n\nPlease remove the USB device an log on again.

With the following two variables you can show a link, for example to display more information about your USB policy. When you click on the link, the specified URL is called in the default browser:

TextUsbLink=More information
UsbLink=http://intranet.mycompany.com/usb

Define your own text to be displayed when an additional keyboard is connected (if KeyboardInstall=warn or block). „\n“ for a new line:

TextKeyboardWarning1=Warning
TextKeyboardWarning2=An unknown keyboard was detected on your computer. If the connected device is NOT a keyboard, but for example a USB stick, you should immediately disconnect it!\n\nIf it is a desired keyboard, please ask your administrator to allow it in USBSecure.
TextKeyboardUnlockLink=Enable additional keyboard
TextKeyboardConfirmButton=Confirm
TextKeyboardUnlock=You are allowed to enable an additional keyboard.\n\nWould you like to enable the keyboard now?
TextKeyboardMsg=Your computer has been locked because of an unknown keyboard. Please disconnect the most previously connected device!\n\nInformation: USB devices, emulating a keyboard, can be a risk for your computer and your network.

You can display a link with the following settings, e.g. to show additional information about bad USB devices:

TextKeyboardLink=More information
KeyboardLink=http://intranet.mycompany.com/usb

InstallLanguage=0409

USBSecure detects the operating system language automatically – on the basis of the registry value InstallLanguage under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language. This value in USBSecure.ini overwrites this setting.

AdminsCantStop=<yes|no>

Determines the right for administrators to stop the USBSecure service. This setting can also be set during Installation (MSI value ADMINSCANTSTOP=1 or 0). Please note that a change of this value will take 5 minutes (after service startup) to take effect.
In principle, an administrator can of course always terminate a service. He may have to obtain the necessary rights to do so. This setting makes it somewhat more difficult for a user who has administrator rights.

ApplyConfigAfterServiceStartup=<time in minutes>

When you define ApplyConfigAfterServiceStartup=5, the complete device configuration (usb.cfg, cd.cfg, …) will be copied and reapplied 5 minutes after USBSecure service startup. Use this feature in environments where the network is not ready at service startup, for example in VPNs or in NAC environments (Network Access Control). Possible values are: 2 - 999 (0 = off).

ApplyConfigDailyAt=<time>

Use entry ApplyConfigDailyAt=00:30 to copy and apply the complete device configuration (usb.cfg, cd.cfg, …) at 00:30 AM. Use this feature in environments with computers running 7x24. If a computer is not connected to the network or switched off, this task will not be repeated.

BluetoothSupport=<yes|no>

Use entry BluetoothSupport=no to disable Bluetooth support.

DeviceLogging=<yes|no> (only OT version)

Specifies whether a local logging of all plugged in and unplugged devices is to take place in the DeviceLogging.log file.

MinKeyboardCount =<count>

Sets the maximum number of keyboards allowed at the same time to the value <count>. This is the value that will later be in the KeyboardCount.cfg file. Addresses the problem that PCs often do not have a keyboard connected during the operating system installation. The KeyboardCount.cfg file then contains a 0. Set MINKEYBOARDCOUNT=1 so that there is at least a 1.

AdminGuiLogging=<yes|no>

By default, actions performed with the USBSecure Admin GUI are logged in the Devices$\Backup\USBSecure-Admin.log file. If this is not desired, it can be disabled with AdminGuiLogging=no.

Example configurations USBSecure.ini

1. You want the blue warning message to appear and the computer to be locked when USB mass storage devices are plugged in that are not allowed in the usb.cfg file (the user can log in again immediately). Unknown smartphones and digital cameras should be disabled without notification. Configure the following values in USBSecure.ini for this purpose:

   → NoUsbStorInfo=no
   → SmartphoneInfo=no

2. You want the blue warning message to appear for inserted USB mass storage devices that are not allowed in the usb.cfg file, but the computer should not be locked. Unknown smartphones and digital cameras should be disabled without notification. Configure the following values in USBSecure.ini for this purpose:

   → NoUsbStorInfo=warn
   → SmartphoneInfo=no

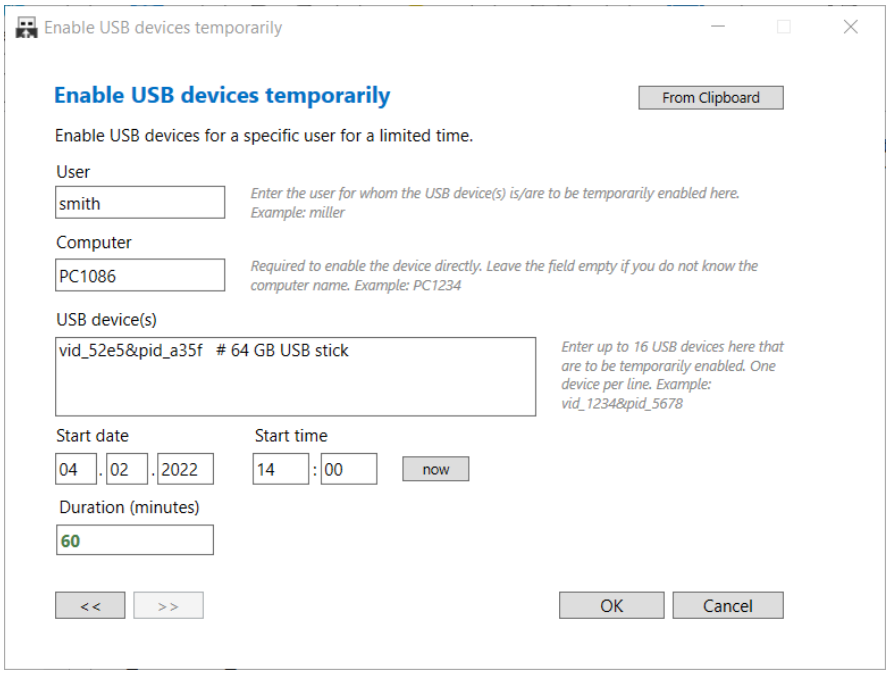
3. You want the blue warning message to appear for inserted USB mass storage devices that are not allowed in the usb.cfg file, but the computer should not be locked. The same should happen with unknown smartphones and digital cameras. Configure the following values in USBSecure.ini for this purpose:

   → NoUsbStorInfo=warn
   → SmartphoneInfo=yes

Enable USB devices temporarily

You can temporarily enable USB devices - for example, a USB stick - for specific users. After the period has expired, the device is automatically deactivated.

To do this, click "Temporary" in the USBSecure Admin or right-click a user on the left and then click "Enable USB device temporarily".



If you specify a computer, the activation will be applied immediately. If you leave the field blank, it will be applied only at the next service start on the target computer. Of course, you can also "Apply to computer" afterwards.

Clicking "From Clipboard" will transfer a suitable text from the clipboard directly into the fields of this dialog. The text can be copied from a notification mail or a notification file (devicesRW$\Notify) to the clipboard.

The "Browse" buttons (<< and >>) can be used to display up to 10 already executed activations.

Mail notification

A mail notification can be sent to the USBSecure administrators when a forbidden USB mass storage device (stick, hard disk) is plugged in. While USBSecure has no real server component, mail notification has to be performed directly from the client – or with a central scheduled task.

Mail notification directly from client

→ Required entries in USBSecure.ini: SmtpServer, MailFrom, MailTo1

When a forbidden USB mass storage device is connected, the client sends a notification to the recipients specified in USBSecure.ini (MailTo1, MailTo2 and MailTo3). Communication is established on port 25. Because no authentication takes place, your clients must be enabled for internal relaying on your mailserver. In some environments this method could fail because relaying is not allowed or virus scan software or firewalls could prevent the clients from sending E-Mails.

Centrally managed mail notification

→ Required entries in USBSecure.ini: UsbStorNotify=yes

When a forbidden USB mass storage device is connected, the client creates a text file in folder devicesRW$\Notify. These files can be used to send mail notifications to the USBSecure administrators with a scheduled task.
Please create a scheduled task named “USBSecure Mail” in Computer Management of a Windows Server, running once a minute and performing the following command:

Action: Programm starten
Program/Script: C:\USBSecure\SmtpSend.exe
Add arguments: <mailserver name> <sender> <recipient> "Unknown USB mass storage device (%COMPUTER%)" -folder:"\\<USBSecure servername>\devicesRW$\Notify"

Therefor copy file SmtpSend.exe in a newly created folder C:\USBSecure on the server.

As soon as a forbidden USB mass storage device is plugged in on a client machine a text file will be created in folder **\\<USBSecure servername>\devicesRW$\Notify**. This text file will be converted into an E-Mail and then moved to folder “done”.

Logfile USBSecure.log

In USBSecure.log all activities are logged (user logons, start of the USBSecure service, enabling/disabling of devices, license messages etc.). The loglevel should be set to “normal“ in production environments. For diagnostic purposes it can be set to “full“. With full logging more detailed information is logged (see chapter USBSecure.ini).

User <LoggedOff>

User <LoggedOff> is logged in the USBSecure.log file any time no user is logged on. User <LoggedOff> can only access the devices listed in the AllUsers section. At the time of logoff (and before logon) all devices not listed in the AllUsers section are disabled. If this behaviour is undesired (e.g. because a USB WLAN adapter is required at logon) you can set “UsbLoggedOffDeactivation=no“ in USBSecure.ini.

Security – Hardening of the system

Finally, to operate USBSecure securely, you should take or verify the following actions:

1. Ensure that no standard user has write permission to the <Server>devices$ share. Only administrators who use the USBSecure Admin to edit configurations need write permissions to this share. Standard users only need read permissions here. You can use NTFS permissions for this task.

2. Make sure that no standard user has write permissions in the local USBSecure directory (usually C:\Program Files (x86)\USBSecure) and its subdirectories. This is equivalent to the Windows default permissions.

3. If you are using a central USBSecure.ini file: The file is located in the \\<Server>\devices$ directory and is extremely important for USBSecure to work. Make sure that even a majority of administrators do not have write access to this file. Unlike the usb.cfg, bluetooth.cfg, etc. files, this file does not need to be modified during daily operation. You can use NTFS permissions for this task.

Fast User Switching

Fast User Switching was first implemented for domain users in Windows Vista. Fast User Switching allows multiple users to log on to a Windows machine the same time.
If USBSecure detects that multiple users have logged on, it turns to „FastUserSwitching“ mode. In “FastUserSwitching“ mode the user-based allowed devices will be deactivated. Only devices listed in the AllUsers section remain activated.