EventTracker
Secure. Comply. Succeed.

USB Monitoring

ET76U15-060/ET76UA15-060

Publication Date: August 21, 2015

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Update: ET76U15-060/ ET76UA15-060

Abstract: This update will have the USB monitoring feature which will allow users to disable all devices except Human Interface Devices.

Who should read this document?

Customers who use v 7.6.

NOTE: Process to be followed after applying the Update.

USB and other devices:

- Go to **EventTracker Control Panel**.
- Double Click the **EventTracker Agent Configuration**.
- Select the **System Monitor tab**.

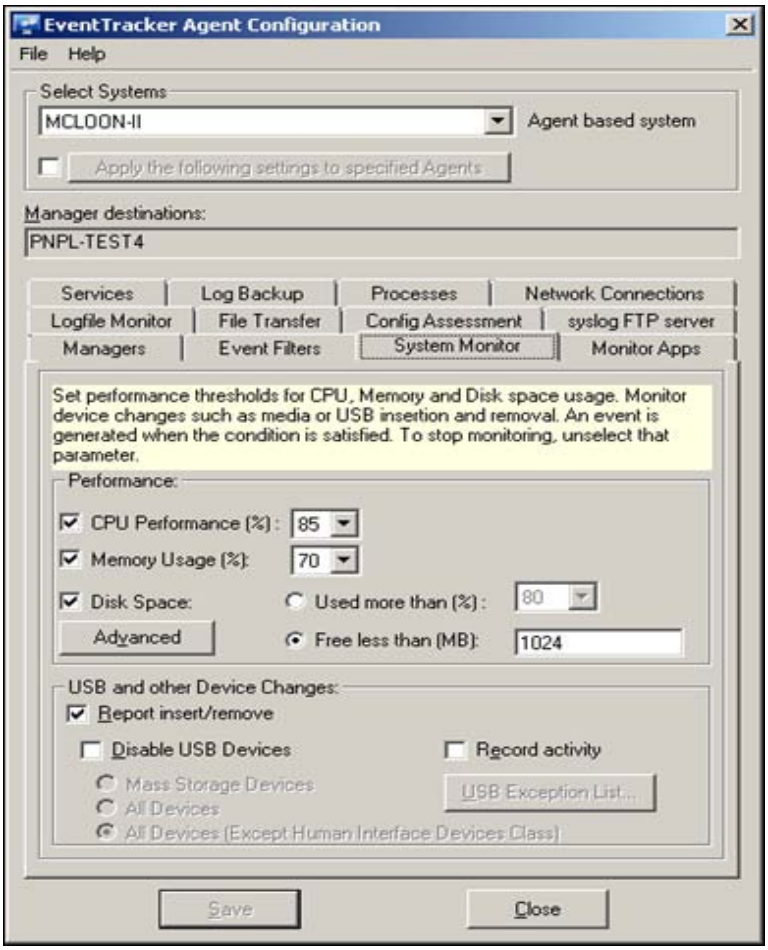

Figure 1

In the **USB and other devices** section,

- **Report insert/remove**

Enable this option to get the device detected and device removal of Event ids 3228 and 3229 for USB/Pen drive/External CDs, DVDs.

NOTE: It will not report device detected and removal for mobile devices/External hard disk/Keyboard/Mouse.

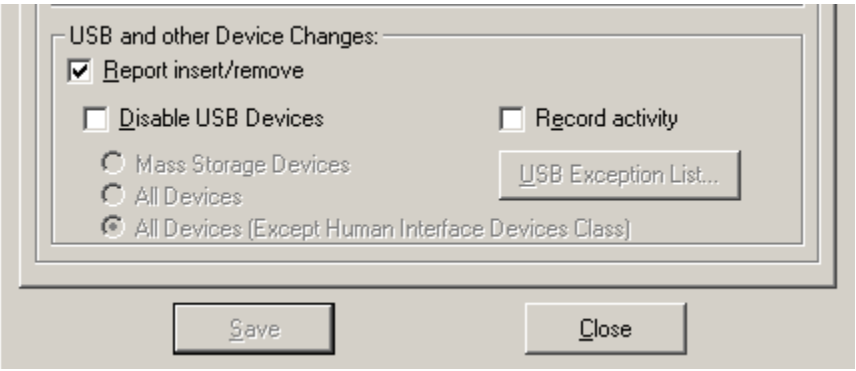

Figure 2

- **Record Activity**

Enabling this option will record add/modify/delete activity from hard disk to external devices. Event id 3240 will be generated. Supported Devices: Pen Drives and CDs, DVDs.

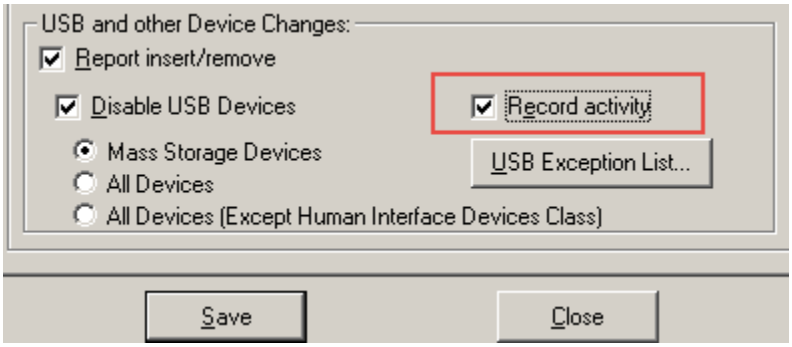

Figure 3

NOTE: It will not record activity for External CDs, DVDs, and mobile devices.

- **Disable USB Devices**

There are sub-options under this option, namely,

a) Mass Storage Devices
b) All Devices
c) All devices (Except Human Interface devices Class)

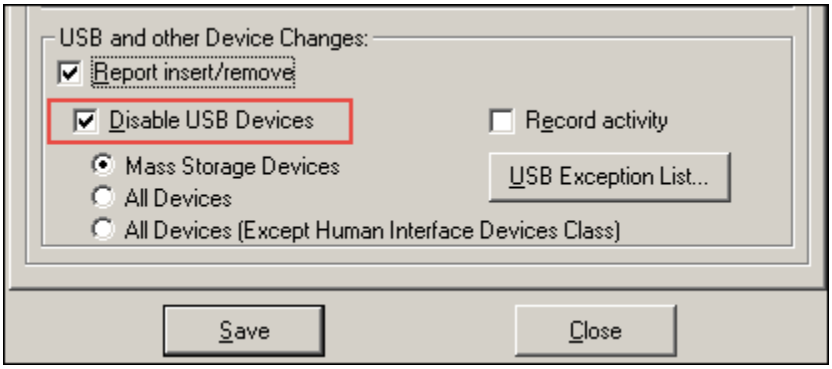

Figure 4

a) Mass Storage Devices

It will disable Pen Drive/External CDs, DVDs/Hard disks and Mobile devices (having Flash Drives and which does not have SD cards), connected as USB storage. For example: Non-Android Mobiles such as sm-b310e and Android mobiles of earlier versions such as 2.0 series.

b) All Devices

It will disable Pen drive/External CDs, DVDs/Mouse/USB Head Phones/ USB External CDs, DVDs **except Keyboard**.

c) All Devices (Except Human Interface Devices Class)

All devices such as Pen drive/External CDs, DVDs/Mouse/USB Head Phones/ USB External CDs, DVDs will be displayed **except Human Interface Devices (HIDs) which includes Keyboard, Mouse, Joystick and Numeric Keypad.**

- **USB Exception list...**

To configure USB exception list, click the **USB Exception List** button.

EventTracker displays the USB Exception List pop-up window.

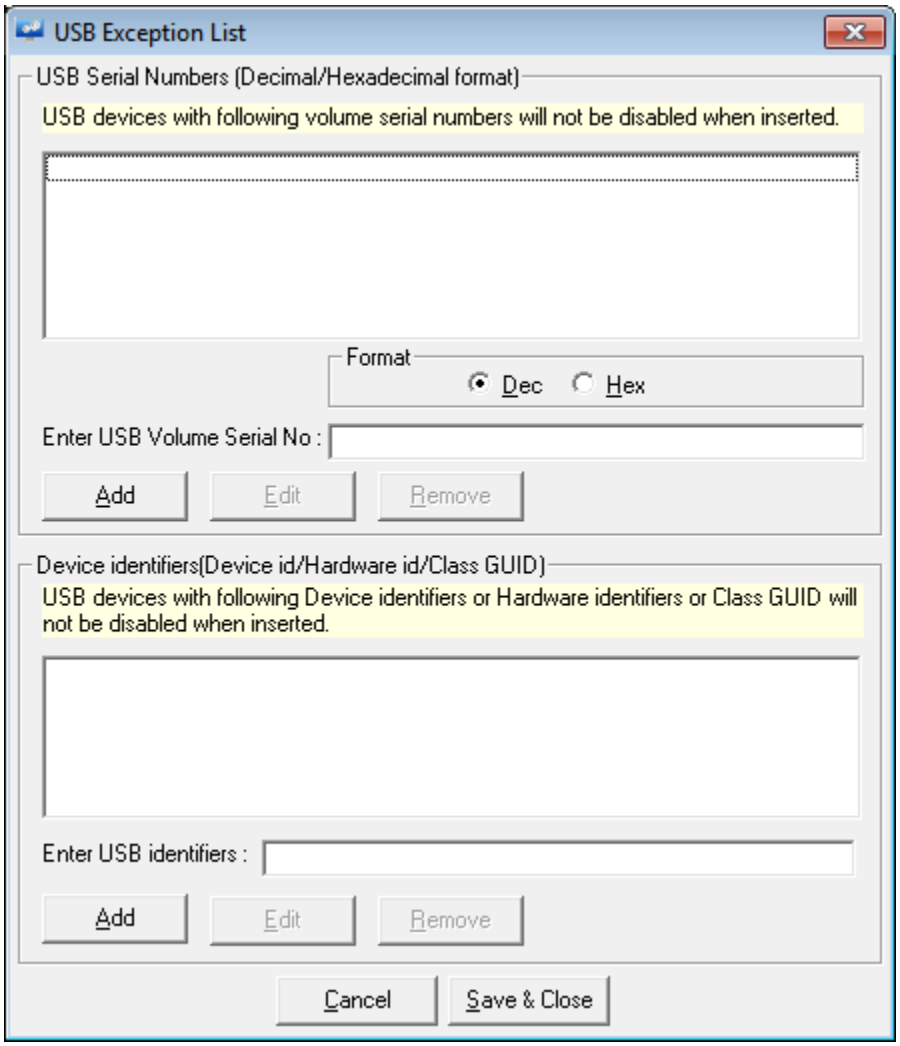

Figure 5

The USB Exception list is parted into two sections:

1. **USB Volume serial Number** section

   It will work for the devices which have volume level such as the Pen Drive.

   - Type the USB serial number in decimal format or hexadecimal format in the **Enter USB Serial Number** field, and then select the **Format** option accordingly.

     OR

   - Type USB device ID in the **Enter USB Device ID** field.

- Click the **Add** button.

EventTracker adds the newly entered Volume serial number in the exception list.

To find **USB volume serial number**,

1. Verify if the USB device is inserted properly on the system.
2. Open **My Computer** and note the drive letter for the USB device.
3. Open the command prompt and change to the USB drive by typing <drive letter>.
4. Type"**dir**" to see the directory listing.

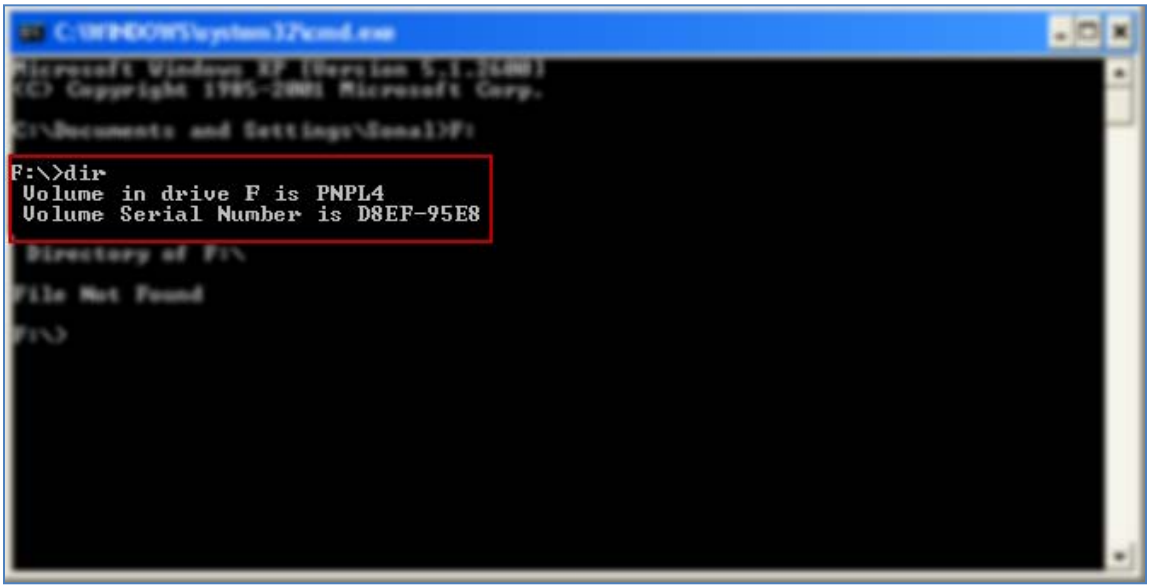

Figure 6: Find the USB serial number in command prompt

5. Note down the volume serial number shown in 'Hexadecimal' format.
6. In the **USB Exception list** window, enter this serial number in **Enter USB Volume Serial number** text box.
7. Click the **Hex** option.
8. Click the **Add** button to add the serial number.

   The output will be seen as below.

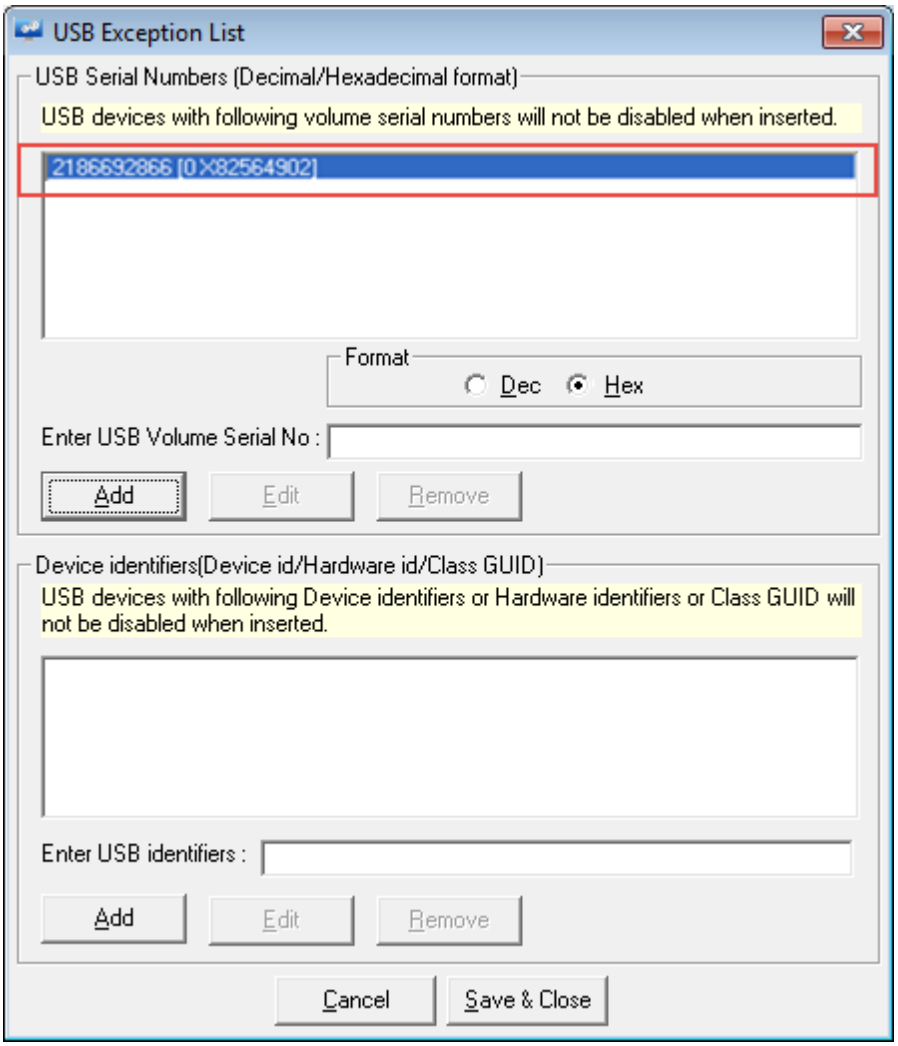

Figure 7

NOTE:

- In the command prompt, the volume serial number will always be in 'Hexadecimal' format. You can convert it into 'Decimal' format, if required.

- **It works only for Pen drive and no other Mass storage devices.**

2. **Device Identifiers** (Device id/ Hardware id/ Class GUID)

   The USB devices with the Device Indentifies- Device id/Hardware id/ Class GUID will not be disabled, when inserted.

   a) **Device id**: It differs for all devices.

For adding Device id to exception list:

- Right click on computer, select **Manage**.

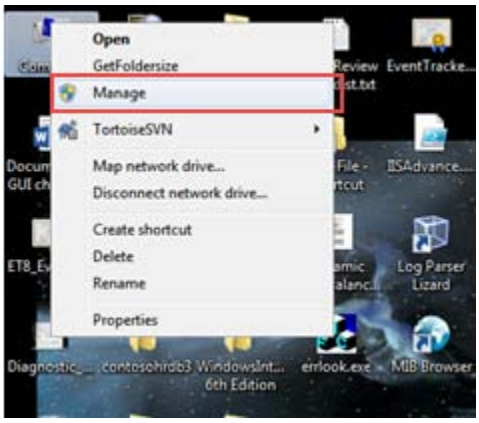

Figure 8

- Select **Device Manager.**

NOTE: Based on the device, select from the listed options.

For Example:

1. The Latest Android mobiles when inserted will display as 'Portable devices '. The screen is displayed below:

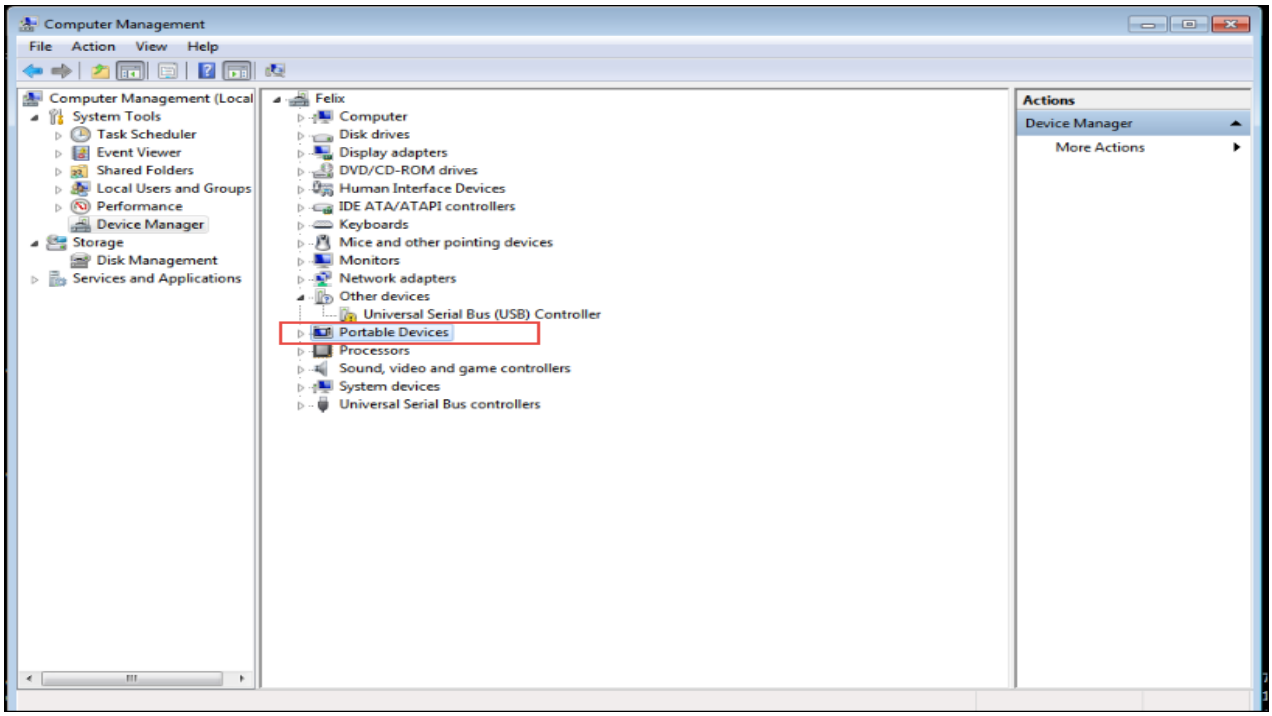

Figure 9

2. The Android mobiles of earlier versions such as 2.0 (having Flash devices), when inserted will display within **USB Mass Storage Device**. Here we have shown example for USB Mass storage Device.

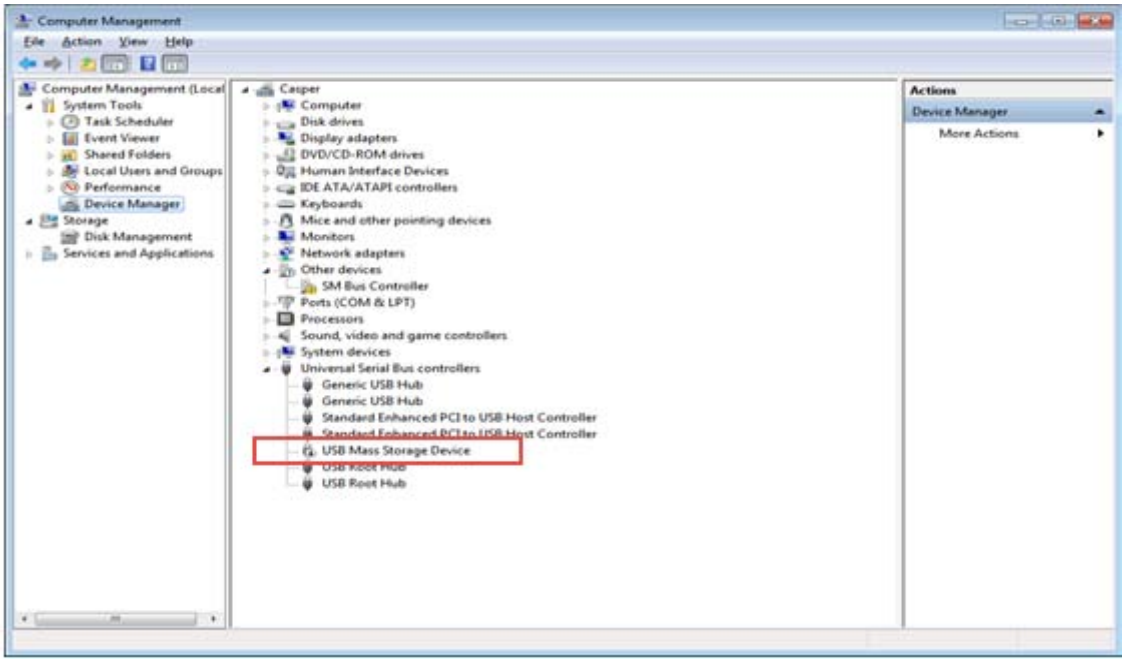

Figure 10

- Right click on **USB Mass Storage device**. Select **Properties**.

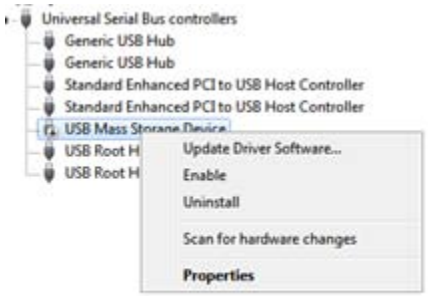

Figure 11

The USB Mass Storage Device Properties display.

- Select the **Detail** tab.
- In **Property** option, select **Device Instance path** from the dropdown list.

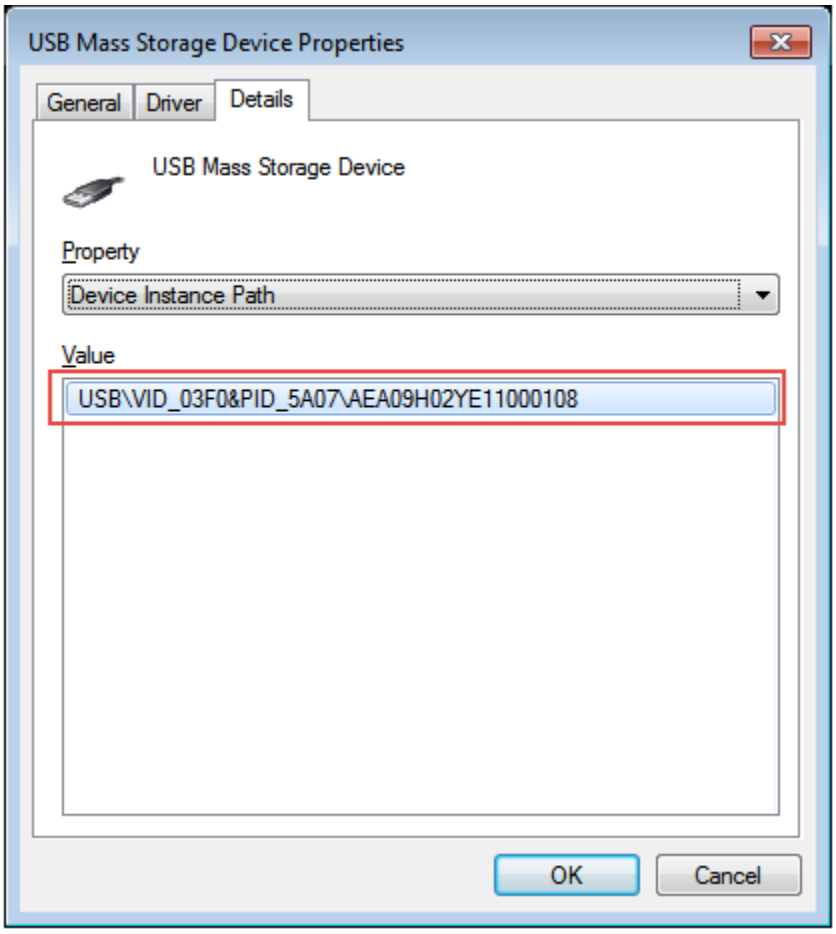

Figure 12

- Copy the **Value:** highlighted in the figure above and paste it in the **Device Identifiers** field as displayed in the figure below:

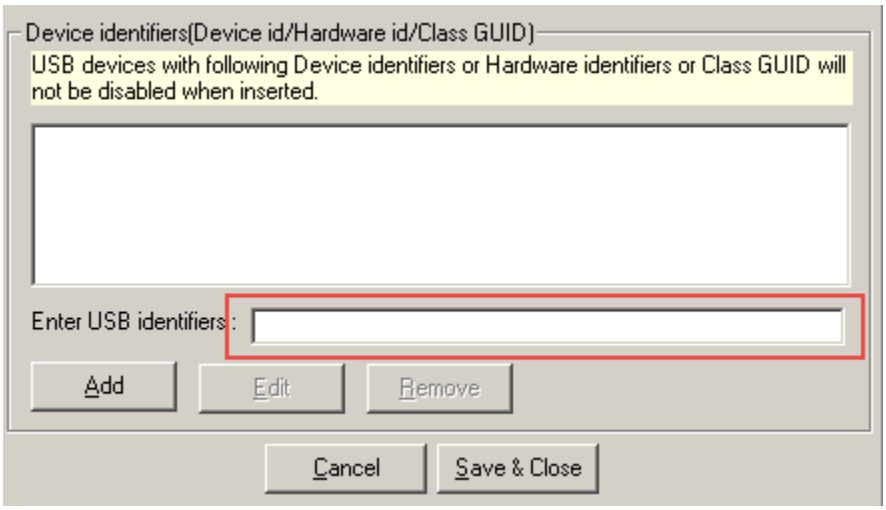

Figure 13

- Click the **Add** button.

It gets added and is displayed.

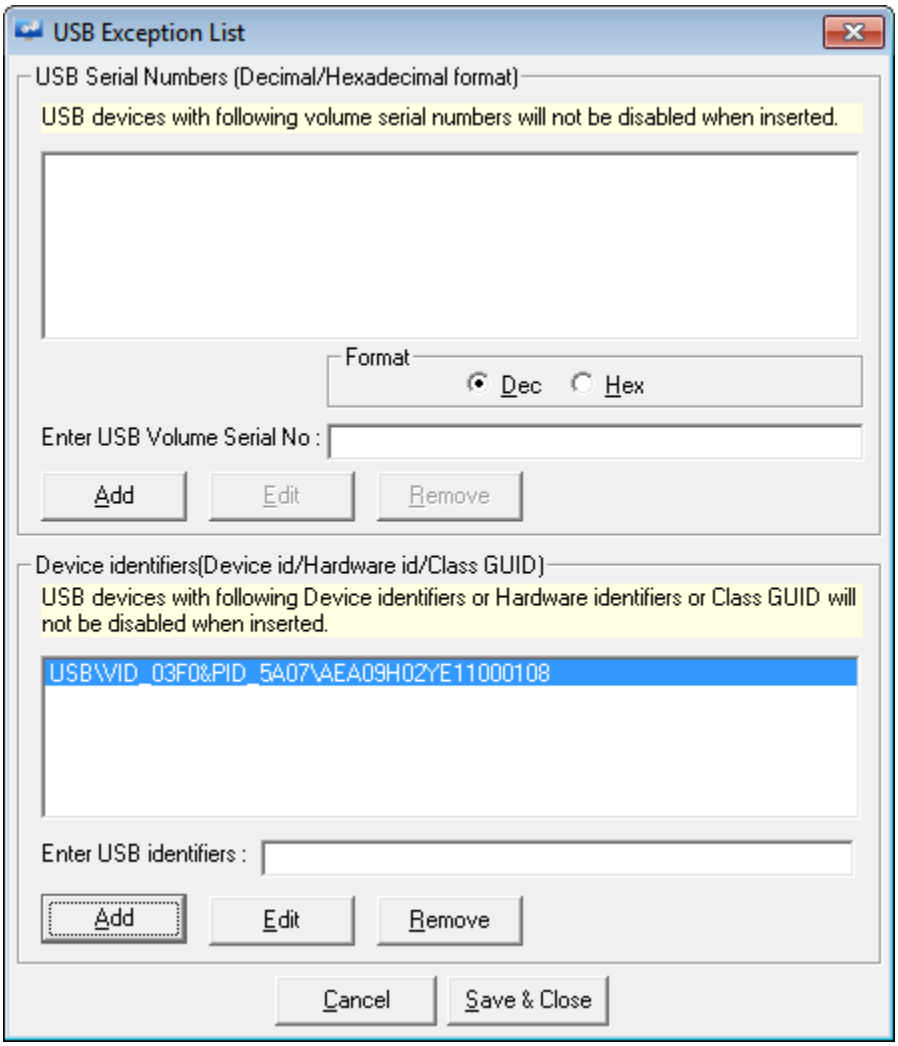

Figure 14

b) Hardware id: Remains same for a particular device of same class type but different for other class type. (e.g. Hardware id of all HP optical mouse will be same , but hardware id of Lenovo, dell or HP will differ from each other)

For adding Hardware id to exception list,

- Select **Hardware id** from the dropdown list in the **Property** option.

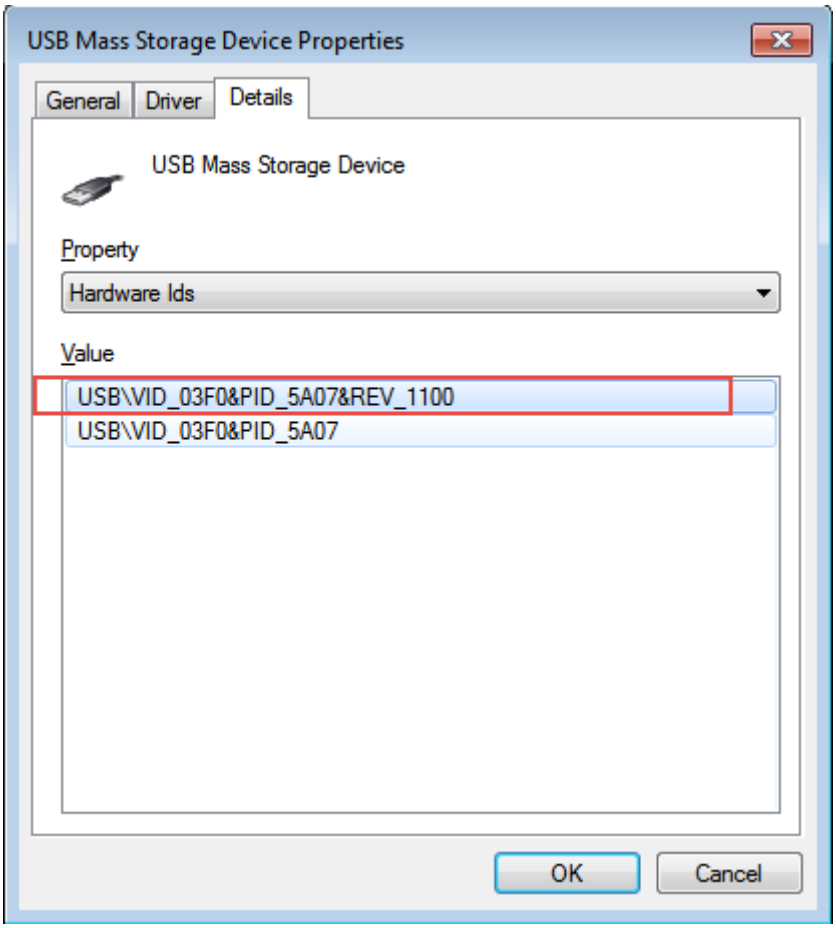

Figure 15

- Copy the value and paste it in the **Device identifiers** field.
- Click the **Add** button.

It gets added and displayed.

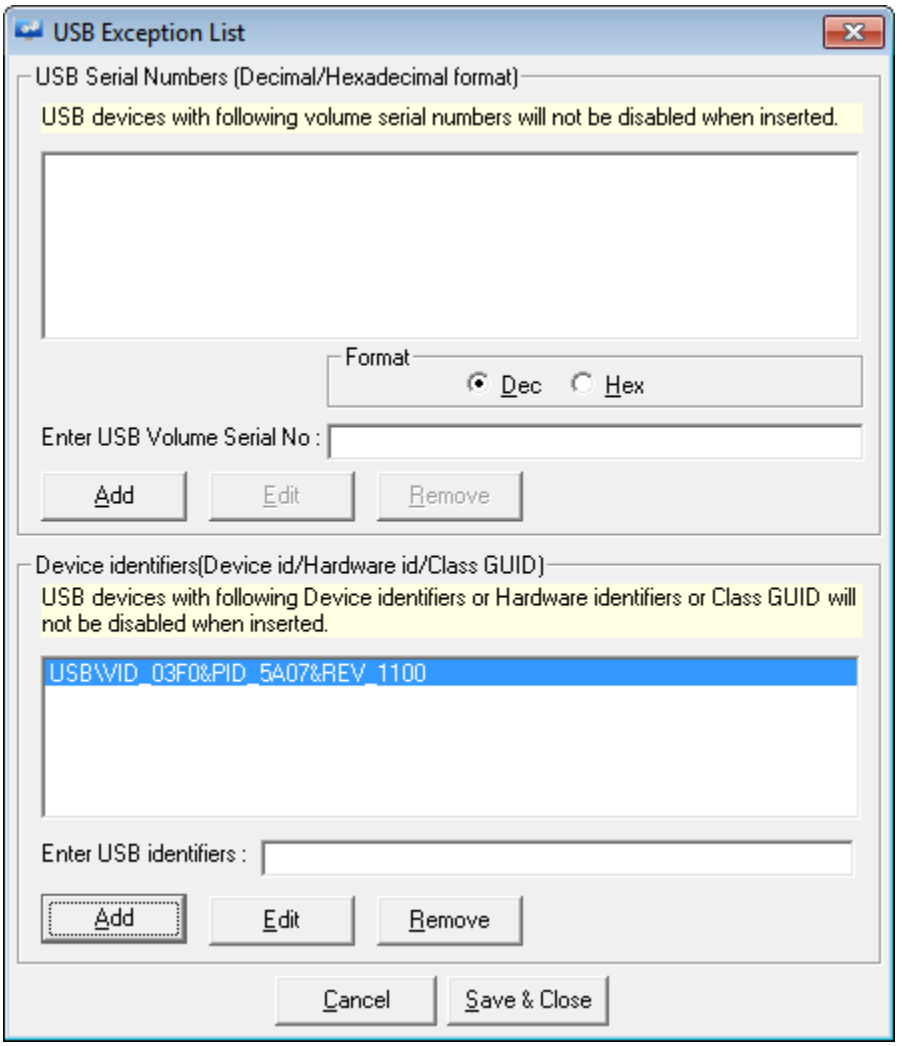

Figure 16

c) **Class GUID**: Remains same for a device class.(e.g. class GUID of optical mouse will be same for all types of mice whether it is Lenovo, dell or HP).

Below displayed, is a table with the devices and their respective values.

Devices	Value
Battery	{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Biometric	{53D29EF7-377C-4D14-864B-EB3A85769359}
Bluetooth	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
CDROM	{4d36e965-e325-11ce-bfc1-08002be10318}
DiskDrive	{4d36e967-e325-11ce-bfc1-08002be10318}
Display	{4d36e968-e325-11ce-bfc1-08002be10318}

Devices	Value
FDC	{4d36e969-e325-11ce-bfc1-08002be10318}
FloppyDisk	{4d36e980-e325-11ce-bfc1-08002be10318}
HDC	{4d36e96a-e325-11ce-bfc1-08002be10318}
HIDClass	{745a17a0-74d3-11d0-b6fe-00a0c90f57da}
Dot4	{48721b56-6795-11d2-b1a8-0080c72e74a2}
Dot4Print	{49ce6ac8-6f86-11d2-b1e5-0080c72e74a2}
61883	{7ebefbc0-3200-11d2-b4c2-00a0C9697d07}
AVC	{c06ff265-ae09-48f0-812c-16753d7cba83}
SBP2	{d48179be-ec20-11d1-b6b8-00c04fa372a7}
1394	{6bdd1fc1-810f-11d0-bec7-08002be2092f}
Image	{6bdd1fc6-810f-11d0-bec7-08002be2092f}
Infrared	{6bdd1fc5-810f-11d0-bec7-08002be2092f}
Keyboard	{4d36e96b-e325-11ce-bfc1-08002be10318}
MediumChanger	{ce5939ae-ebde-11d0-b181-0000f8753ec4}
MTD	{4d36e970-e325-11ce-bfc1-08002be10318}
Modem	{4d36e96d-e325-11ce-bfc1-08002be10318}
Monitor	{4d36e96e-e325-11ce-bfc1-08002be10318}
Mouse	{4d36e96f-e325-11ce-bfc1-08002be10318}
Multifunction	{4d36e971-e325-11ce-bfc1-08002be10318}
Media	{4d36e96c-e325-11ce-bfc1-08002be10318}
MultiportSerial	{50906cb8-ba12-11d1-bf5d-0000f805f530}
Net	{4d36e972-e325-11ce-bfc1-08002be10318}
NetClient	{4d36e973-e325-11ce-bfc1-08002be10318}
NetService	{4d36e974-e325-11ce-bfc1-08002be10318}
NetTrans	{4d36e975-e325-11ce-bfc1-08002be10318}
SecurityAccelerator	{268c95a1-edfe-11d3-95c3-0010dc4050a5}
PCMCIA	{4d36e977-e325-11ce-bfc1-08002be10318}
Ports	{4d36e978-e325-11ce-bfc1-08002be10318}
Printer	{4d36e979-e325-11ce-bfc1-08002be10318}
Processor	{50127dc3-0f36-415e-a6cc-4cb3be910b65}
SCSIAdapter	{4d36e97b-e325-11ce-bfc1-08002be10318}
Sensor	{5175d334-c371-4806-b3ba-71fd53c9258d}
SmartCardReader	{50dd5230-ba8a-11d1-bf5d-0000f805f530}
Volume	{71a27cdd-812a-11d0-bec7-08002be2092f}
System	{4d36e97d-e325-11ce-bfc1-08002be10318}
TapeDrive	{6d807884-7d21-11cf-801c-08002be10318}
USB	{36fc9e60-c465-11cf-8056-444553540000}
Windows CE USB ActiveSync Devices (WCEUSBS)	{25dbce51-6c8f-4a72-8a6d-b54c2b4fc835}

NOTE: By providing the below device values, you can avoid the disabling of the mobile devices.

Device	Value
Windows Portable Devices (WPD)	**{eec5ad98-8080-425f-922a-dabf3de3f69a}**
USB	**{36fc9e60-c465-11cf-8056-444553540000}**

For References: https://msdn.microsoft.com/en-us/library/ff553426(VS.85).aspx

For adding Class GUID in exception list,

- Select Device Class GUID from the dropdown list.

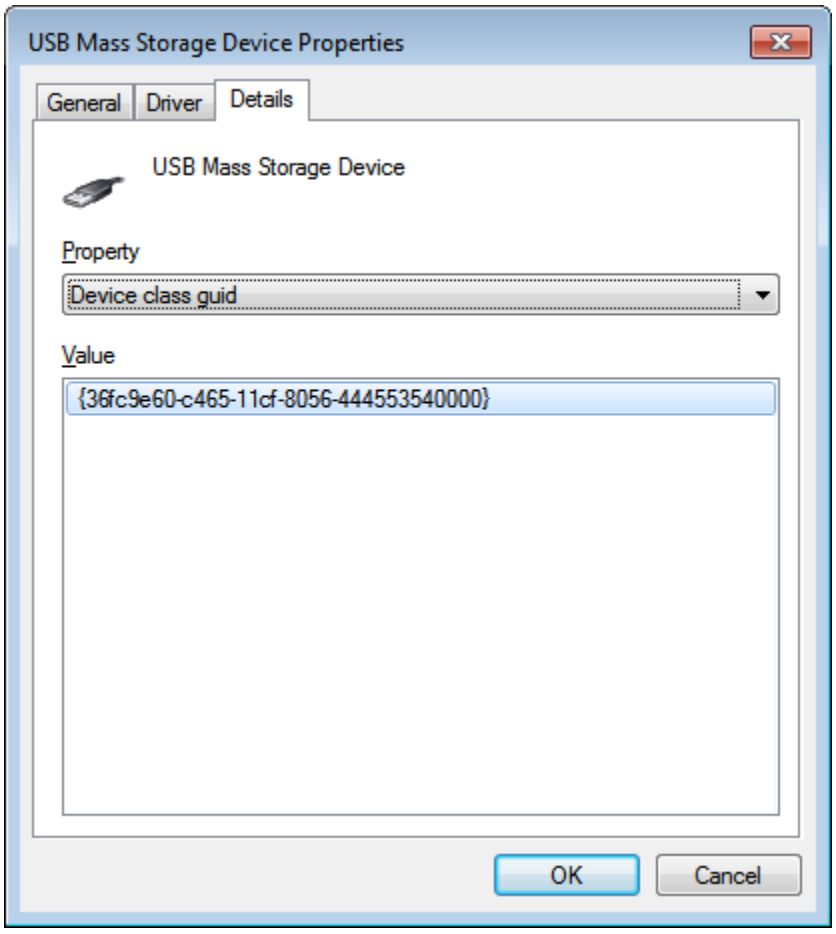

Figure 17

- Copy and paste and the Value: in the **Device Identifier** field.

- Click the **Add** button.

It gets added and displayed as shown in the figure below:

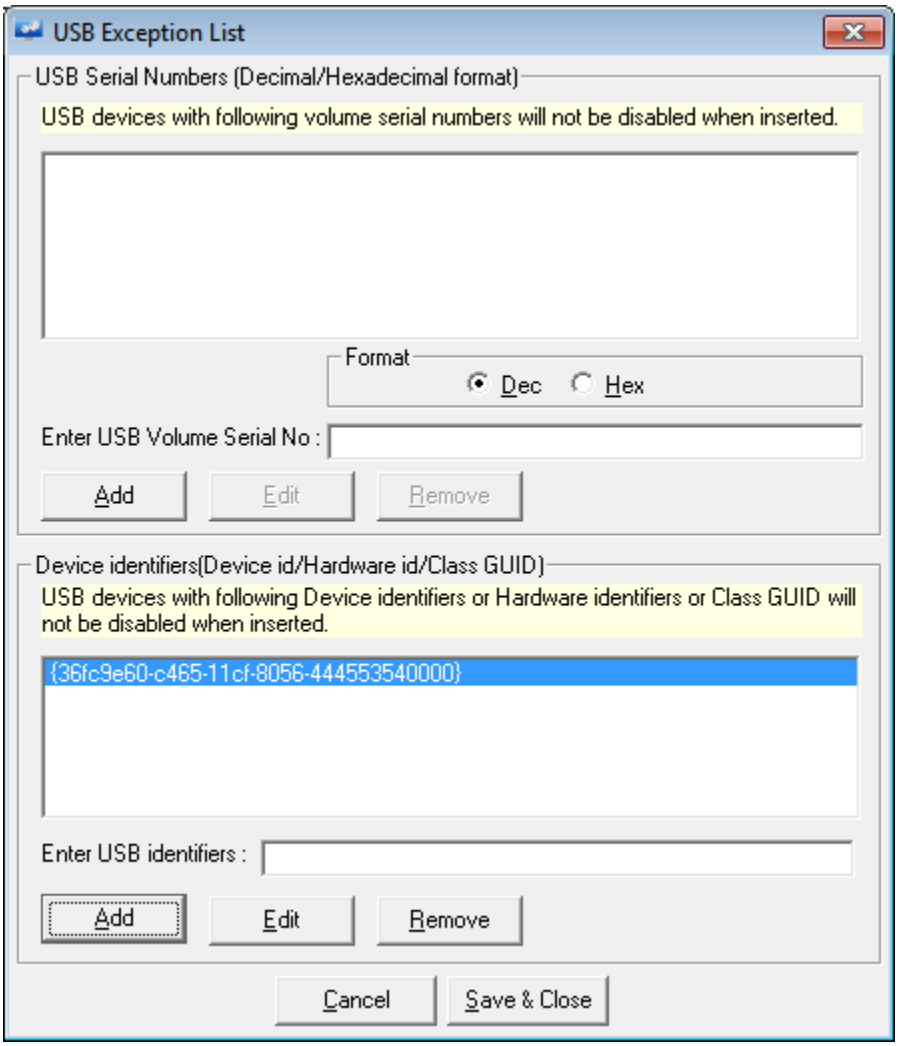

Figure 18

Event description and Event IDs for USB Monitoring

Event description provided by source EventTracker	Event Id
USB Monitoring started for<drive name>	**3239**
USB Monitoring stopped for<drive name>	**3240**
USB device is disabled by EventTracker	**3242**
EventTracker detected new drive	**3228**
EventTracker <drive name> removed	**3229**

EventTracker Web Console

The user can also avail the USB monitoring option from the EventTracker Web Console.

- For this, login to **EventTracker Enterprise**.
- Click on Admin dropdown and select **Windows Agent Configuration.**
- Click on **System Monitor** tab.

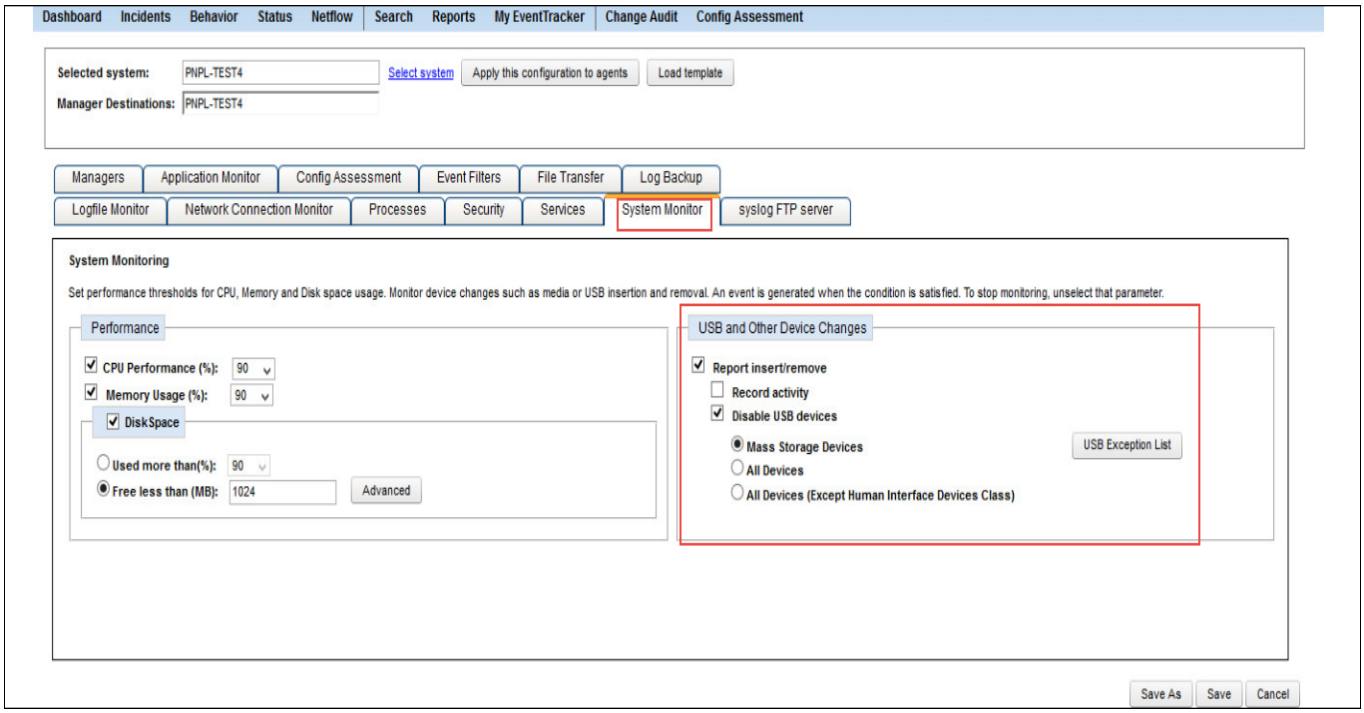

Figure 19

- Click the **USB Exception List** button.

The USB Exception List window displays.

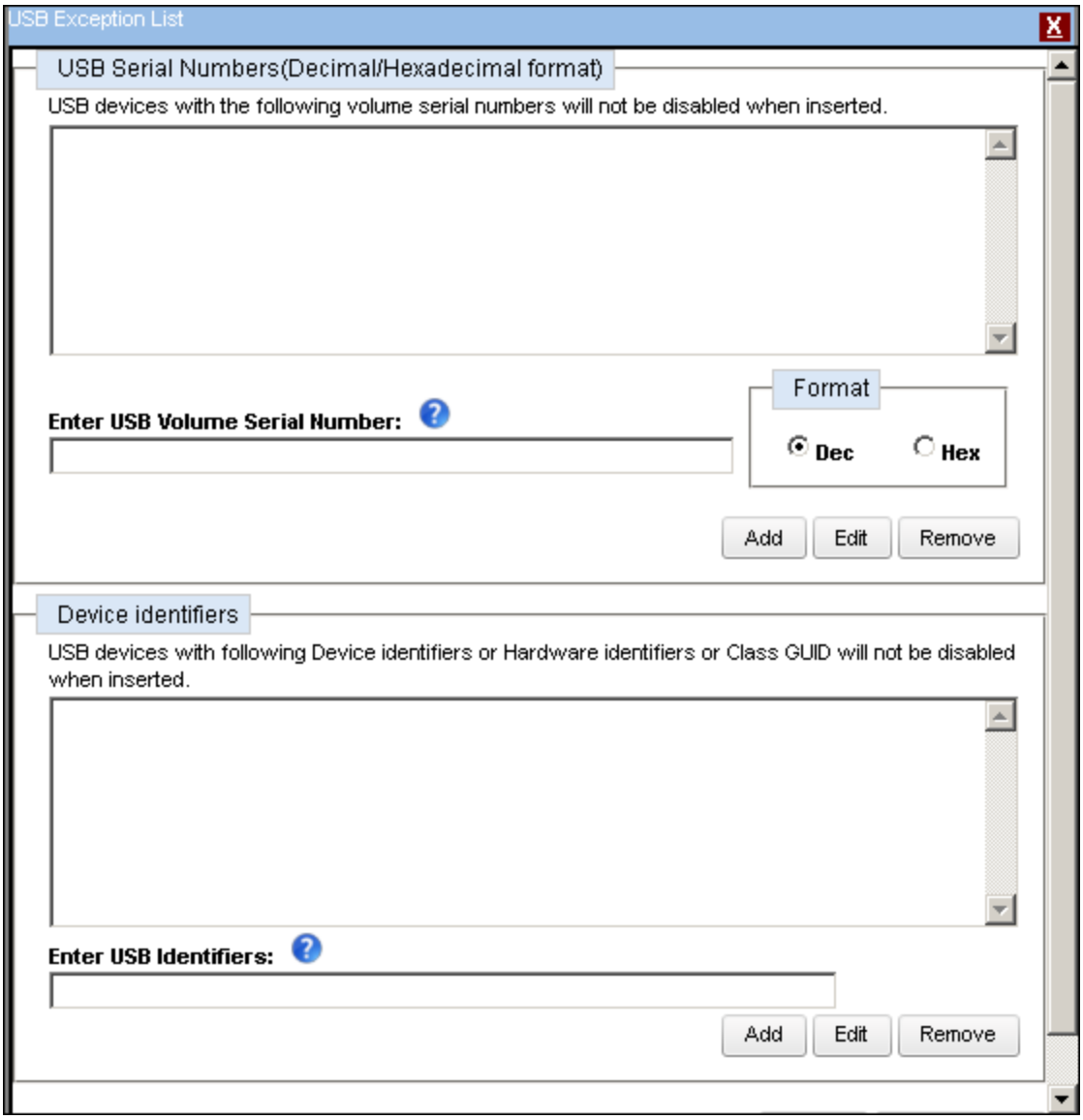
USB Exception List
USB Serial Numbers(Decimal/Hexadecimal format)
USB devices with the following volume serial numbers will not be disabled when inserted.
Enter USB Volume Serial Number:
Format
Dec
Hex
Add
Edit
Remove
Device identifiers
USB devices with following Device identifiers or Hardware identifiers or Class GUID will not be disabled when inserted.
Enter USB Identifiers:
Add
Edit
Remove

Figure 20

Frequently Asked Questions

1. **How to disable all devices using USB Monitoring?**

   Go to **EventTracker Control Panel> EventTracker Agent Configuration>System Monitor** tab, enable the checkbox **Disable USB Devices** and select the option **All Devices.**

2. **How to disable all devices except Human Interface Devices (HID) using USB Monitoring?**

   For disabling all devices except Human Interface Devices, click the option **All Devices (Except Human Interface Device Class)**

3. **How to get the device id/Hardware id/ Class GUID of any specific device?**

   For Example: If we want to get the hardware id for a mobile device (with latest android version),

   - Right click on **Computer.**
   - Select **Manage> Device Manager.**
   - Right click on **Portable device** and select **Properties.**

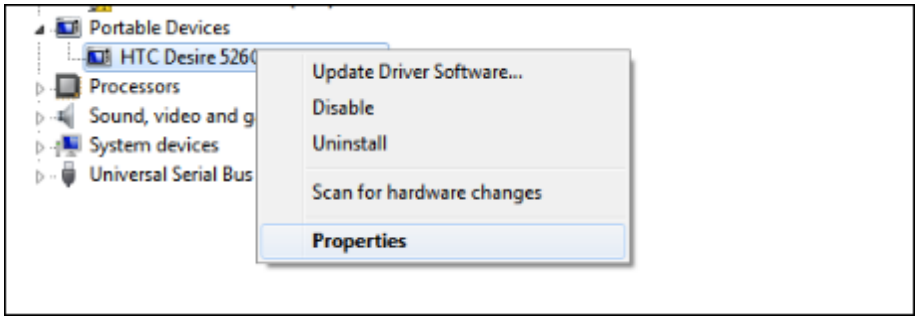

Figure 21

   - In the **Properties** window, click the **Detail** tab.
   - Select **Hardware id** from dropdown list in **Properties** option.

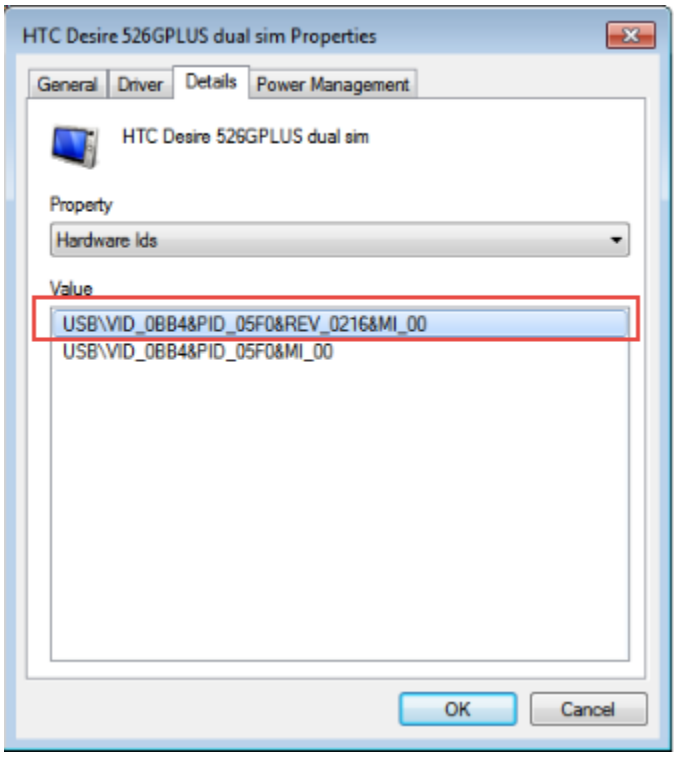

Figure 22

4. How to add mobile devices to the exception list?

Taking the above example, to add the mobile device in the exception list,

- Go to **EventTracker Control Panel> EventTracker Agent Configuration.**
- Select the **System Monitor** tab.
- Click the **USB Exception list** button.

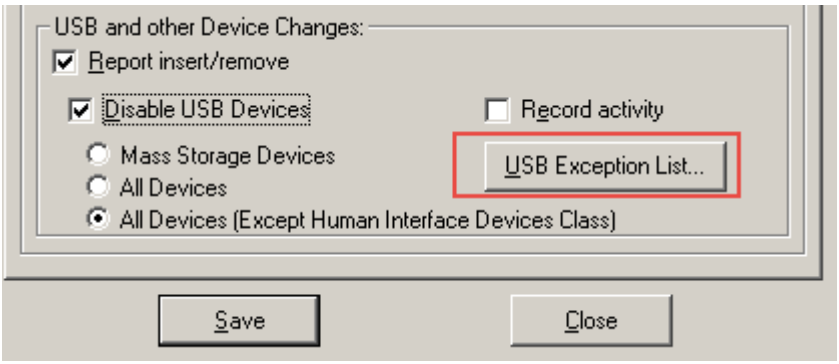

Figure 23

The USB Exception List displays.

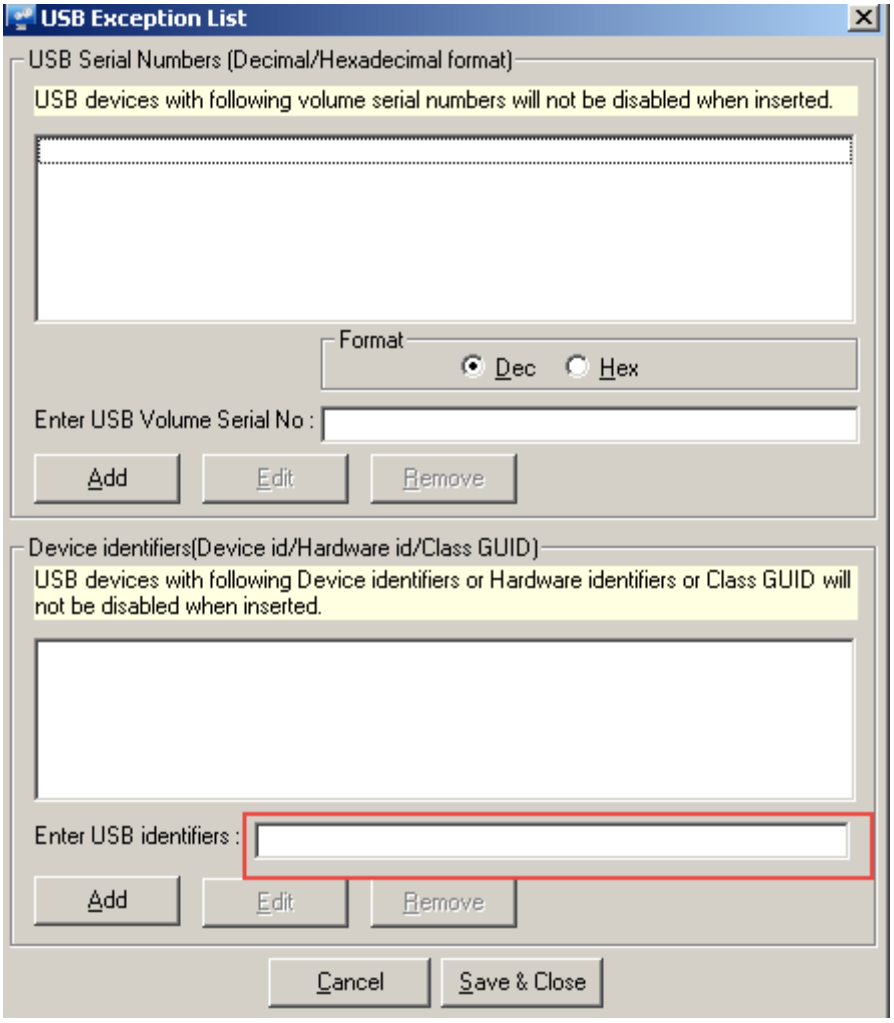

Figure 24

- Copy the Value: (Refer to figure 22) and paste it in **the USB Identifiers** field as highlighted above.
- Click the **Add** button.

It gets added and displayed as shown in the figure below:

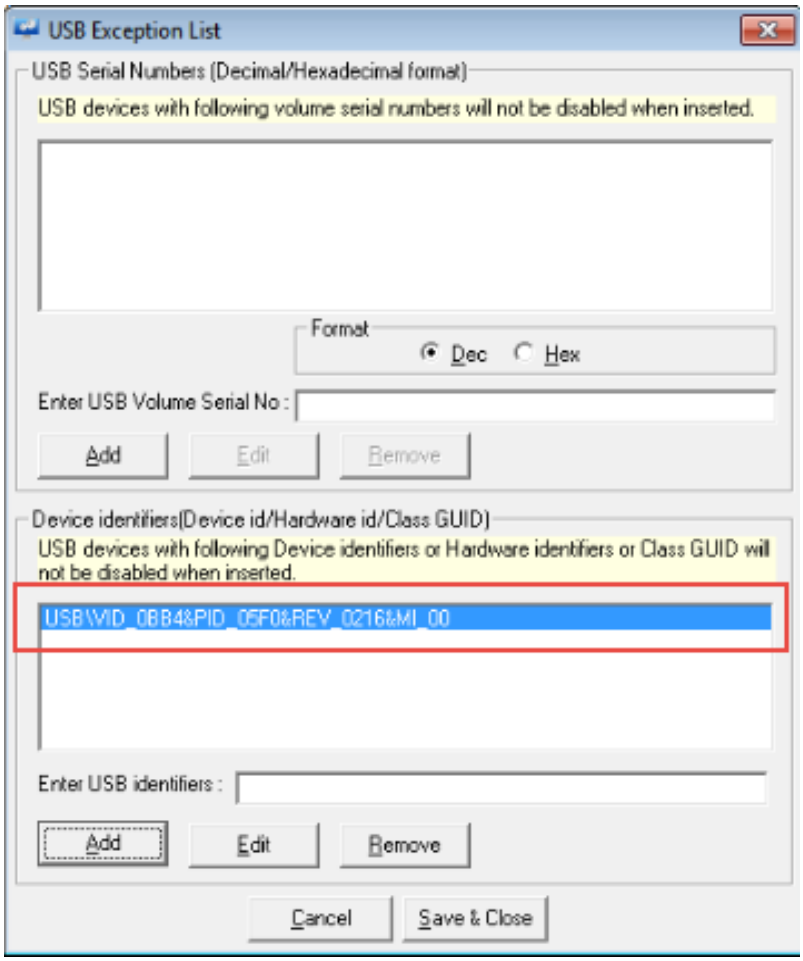

Figure 25: **To exclude disabling of a Specific Mobile Device.**

To exclude disabling of All Mobile Devices using **Class GUID** as Device Identifier,

- Add the below Values in the **USB Exception list** as displayed in the Figure 26.

Windows Portable Devices (WPD)	**{eec5ad98-8080-425f-922a-dabf3de3f69a}**
USB	**{36fc9e60-c465-11cf-8056-444553540000}**

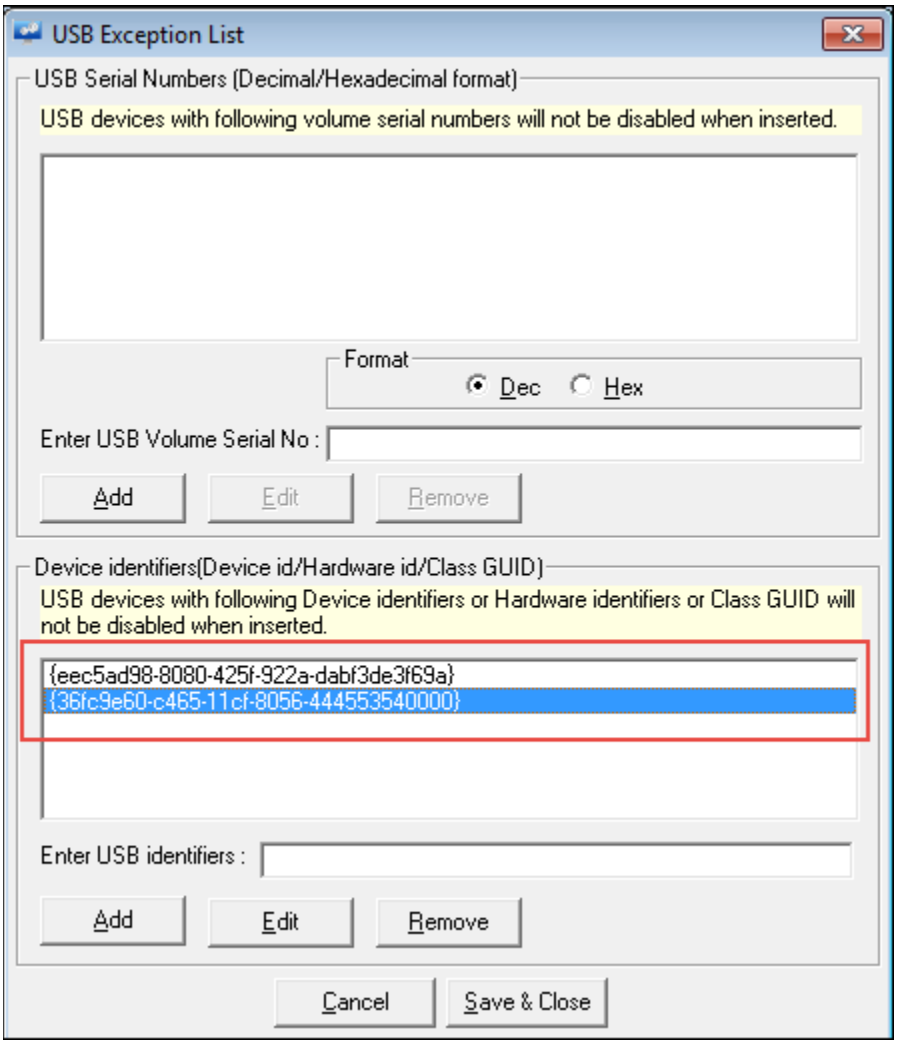

Figure 26: **To exclude disabling of all Mobile Devices (For Class GUID)**