Netsurion | EventTracker®

Removable Media Device Monitoring

EventTracker Version 9.x

Publication Date: November 7, 2019

Abstract

This document will help you to enable the removable device monitoring feature in EventTracker v9.x and explains the procedure of monitoring the activities of the various removable media.

Monitoring when users are attaching external/removable devices (USB, CDs, DVDs) to your systems is an essential component of regulatory requirements and IT best practices. With the introduction of newer portable devices, the security needs of protecting the integrity and confidential data have been changed. An increasing need for portable access to the data has also increased the risk of sensitive or confidential data exposure. Whatever data you are protecting, you need to protect from insider misuse. Therefore, to monitor removable media device activities has become one of the most important compliance factors for the enterprise. EventTracker's advanced removable media monitoring feature protects and monitors system(s) from illegal access or data theft. It delivers essential threat detection and compliance capabilities to detect suspicious or malicious activity before any data loss. EventTracker helps the user(s) to disable the unauthorized access to the machine and allows the connection of the trusted device.

Audience

Administrators who are assigned the task to monitor and manage events using EventTracker.

Table of Contents

1.Overview

The USB and removable media are a vital part of any enterprise for data transfer. They have many forms as flash memory drives, cell phones, cameras, and PDAs that can serve as storage devices. These portable devices are convenient for the transfer and storage of large data with or without network access and quickly too. However, with these advantages, it has some security vulnerabilities. In the modern-day enterprise, USB data transfer is the simplest way of data theft. The chances of data leakage, creation of duplicate documents and illegal data transfer, etc have also increased.

As a SIEM solution, EventTracker not only can monitor the USB or removable media device communications, but it also can identify the trusted USB and other devices. You can define the unique identifier number of the USB so that the device will not be disabled upon insertion, and can access the information from the system.

2.EventTracker Monitoring Features

2.1 Reports insertion/removal of the removable device

EventTracker will log every activity of the USB or other removable media devices like a plug-in, plug-out, or data transfer, etc. A complete audit trail that consists of the user, device type, serial number, time and all the file activities are captured and sent as an event to the EventTracker Console for processing.

2.2 Prevents unauthorized access and reports the intrusion in real-time

Every time a USB is inserted, the EventTracker agent looks at the USB exception list, and if there is no violation of policy, permits access to the device, while logging the insert activity. If a violation of policy is detected, access is prevented, and the violation is immediately sent to the EventTracker Console. At this point, if access is permitted, EventTracker also begins to monitor all the activities on the device, and every file that is written to or deleted from the device is recorded.

2.3 Restricts Access

EventTracker can restrict access to all the USB Devices on a system and can exempt the specified USB devices from monitoring which are added in the USB Exception list.

2.4 Protects the system from malware

EventTracker can disable the USB or other removable media device upon insertion, and thus safeguards the network from viruses and Trojans.

2.5 Logging USB device communication

For security and compliance purposes, EventTracker logs the USB communication in detail as incidents.

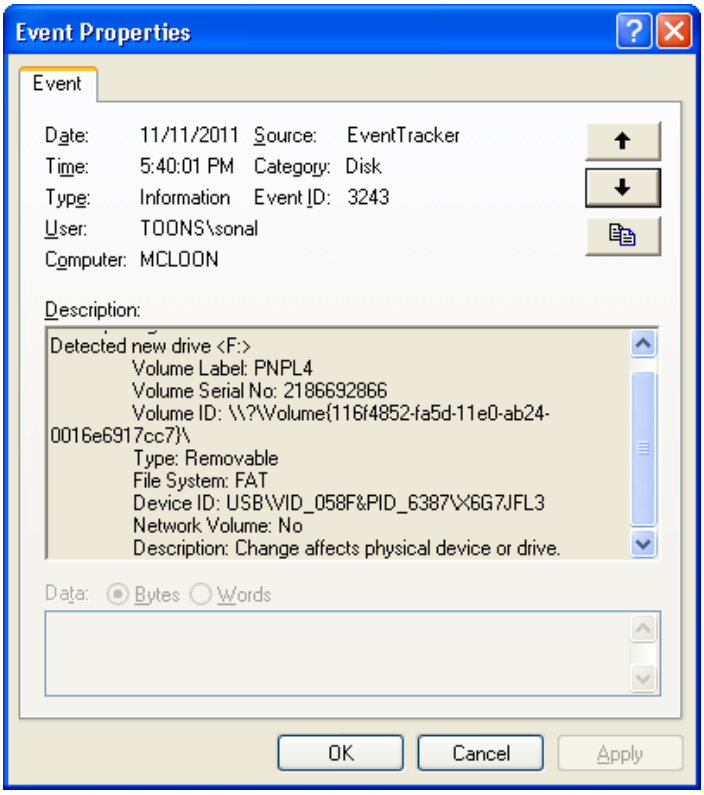


Figure 1

2.6 Get Alert notification

In EventTracker, user can configure alerts to receive the notification upon removable media activities.

Example: EventTracker: USB device disabled, Media Insert alert etc.

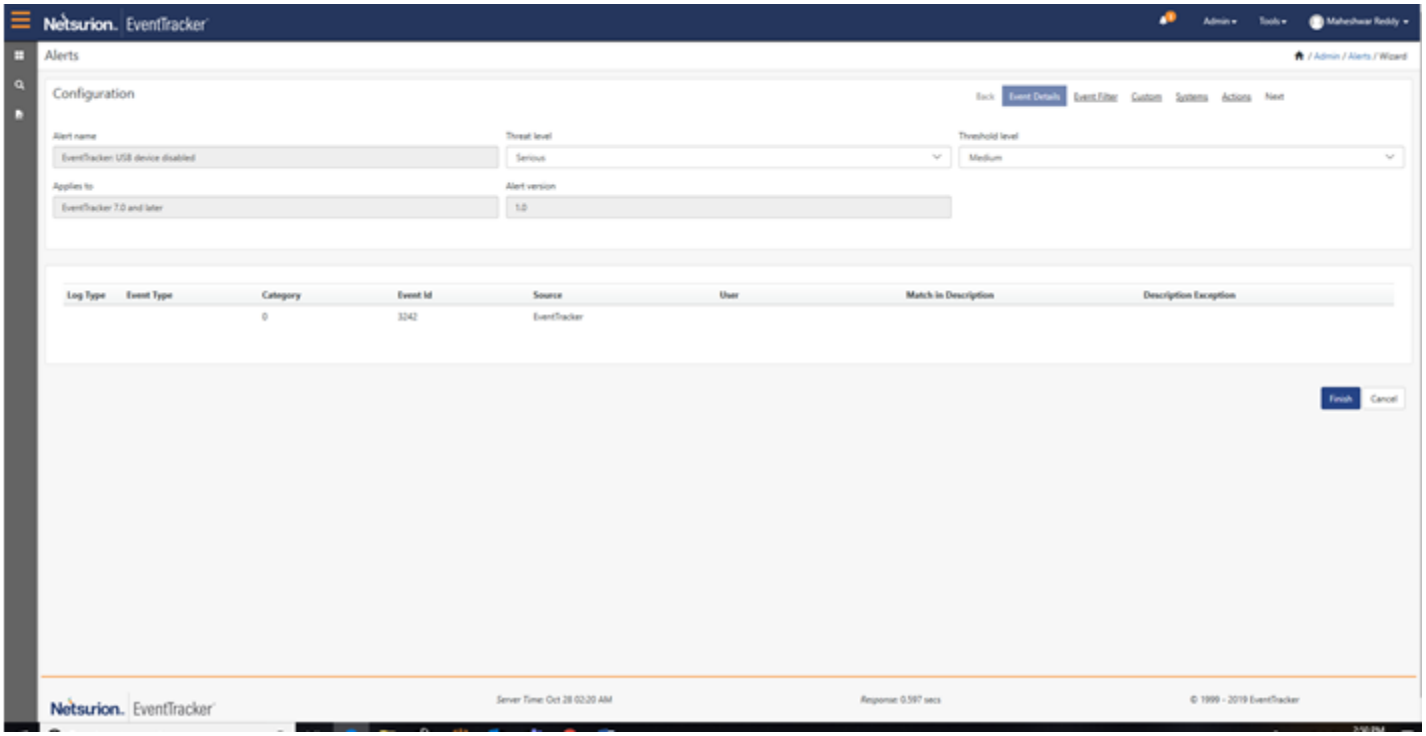


Figure 2

2.7 Configures Media Insertion Report

EventTracker has a provision to configure the reports to analyze the removable media device activities. These reports are helpful to find unauthorized access to the systems. To configure the USB device report, open **EventTracker** >> Click **Operations** menu >> Click **Reports** tab >> In the **Report Tree**, click **USB Device Report** node.

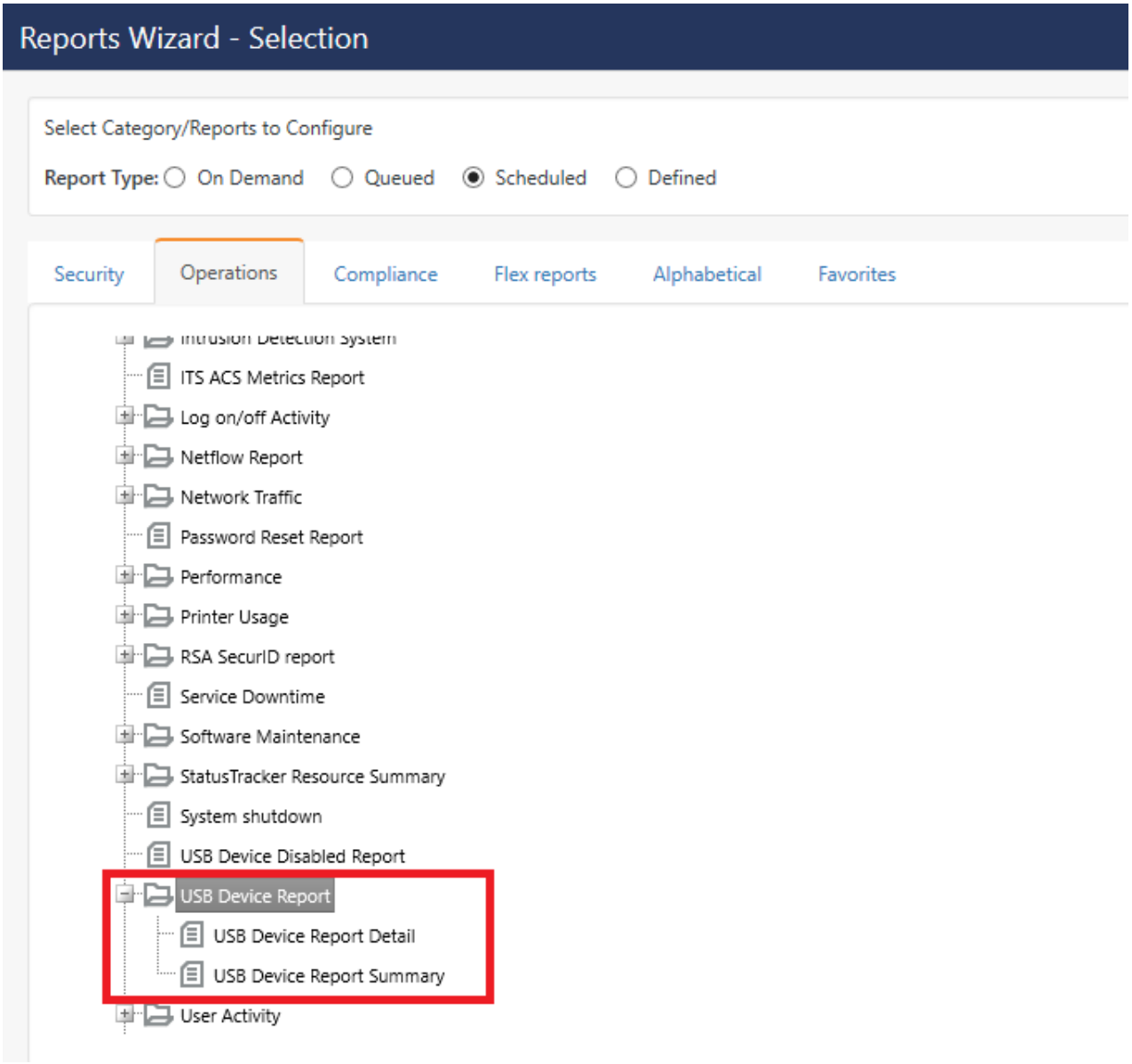


Figure 3

3. Implementing Removable Media Monitoring Feature

1. When a USB device is plugged in or a media is inserted to the CD/DVD drive, Windows sends media insertion notification with the drive letter/name to the EventTracker Windows Agent.
2. Upon receiving the notification, EventTracker Windows Agent launches **USBTracker.exe** with drive details. **USBTracker.exe** is an EventTracker utility that monitors removable media file changes activities.

3. **USBTracker.exe** generates event 3239 and starts monitoring all activities (files added/modified/deleted/copied) that happen on the removable media.
4. When the USB device is unplugged or media is ejected, Windows sends a media removal notification to the USBTracker.exe.
5. Upon receiving the notification, USBTracker.exe stops monitoring and generates event 3240 with details on all activities and exits.

NOTE:

This feature is supported for Windows only and requires EventTracker Agent to be installed and configured.

3.1 Monitoring CDW/DVD Burning Activities

Windows has a built-in CD recorder feature that lets you drag and drop files using Windows Explorer to write files to a CD. Before burning the CD, Windows buffers the files in the 'staging area'. The staging area is a hidden folder that is usually "Drive_letter:\Documents and Settings\Username\Local Settings\Application Data\Microsoft\CD Burning ".

By monitoring the staging area for the list of files being queued up for writing, you can unravel rather a disquieting puzzle who? when? and what?

3.2 Monitoring CD-ROM Activities

Windows copies the files copied from CD-ROM (CTRL + C or mouse right-click) to the clipboard. By monitoring the clipboard, you can keep tabs on the file copy activity.

3.3 Configuring EventTracker Agent to Monitor Removable Media

1. Click the **Admin** drop-down list and then click the **Windows Agent Config**.
2. Select the system from the **Select system** drop-down list.
3. Click the **System Monitor** tab.
   Report insert/remove checkbox is selected by default. Leave as it is.
4. Select the **Record activity** checkbox under **USB and Other Device Changes**.
   This enables monitoring of all removable media (USB, CD-R, CD-RW, and DVD) on the managed system.
5. Click **Save**.

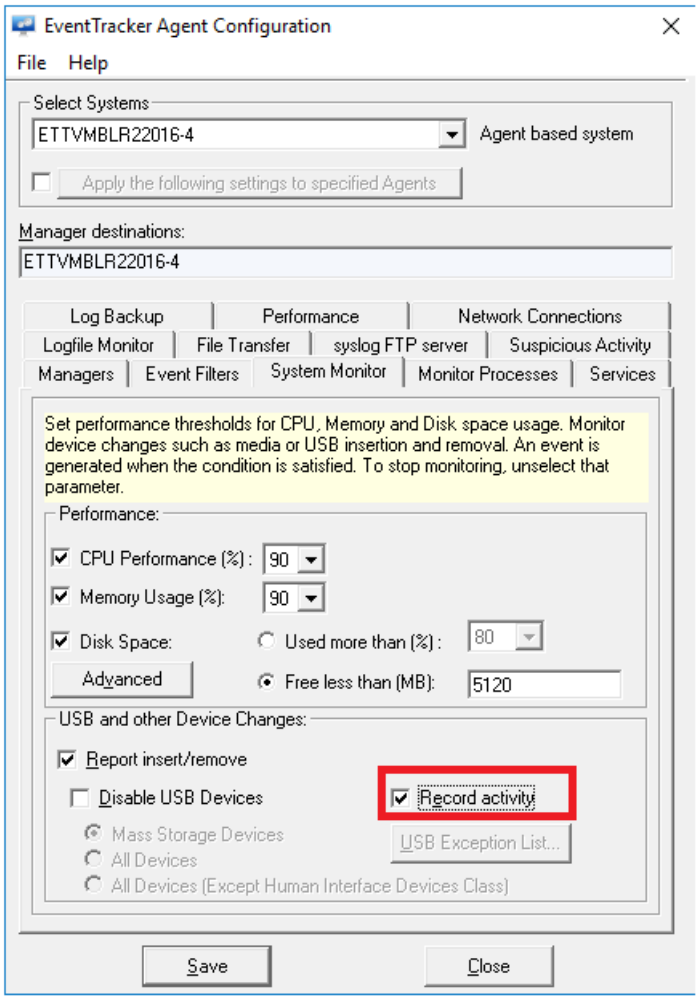


Figure 4

- This option will report 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.

3.3.1 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 5

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

3.3.2 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 6

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.**

4. Exempt Authorized USB Drives

This option helps you restrict users to use only authorized USB devices.

1. Click the **USB Exception List**. EventTracker enables this button only when you select the Disable USB devices check box.
   EventTracker displays the USB Exception List pop-up window.

The USB Exception list is parted into two sections:

4.1 USB Volume serial Number

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

1. Select an appropriate **Format** option.
2. Type the serial number in the **Enter USB Serial number** field.
3. Click **Add**.
   EventTracker adds the newly entered Volume serial number in the exception list.

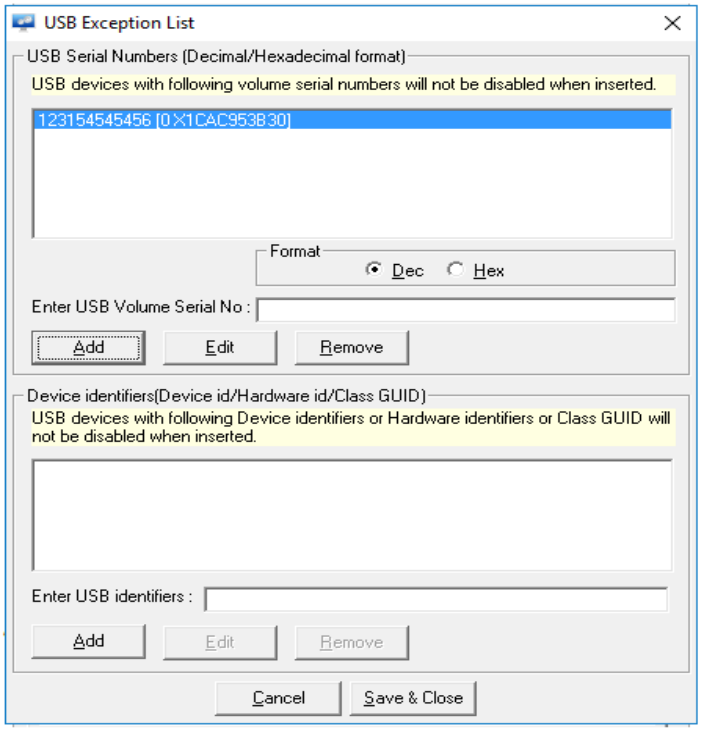


Figure 7

4.2 Finding 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.

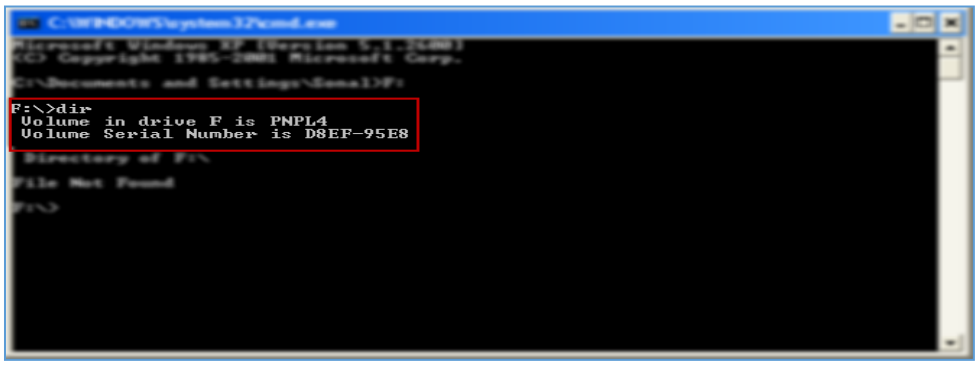


Figure 8

5. Note down the volume serial number shown in the '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 below.

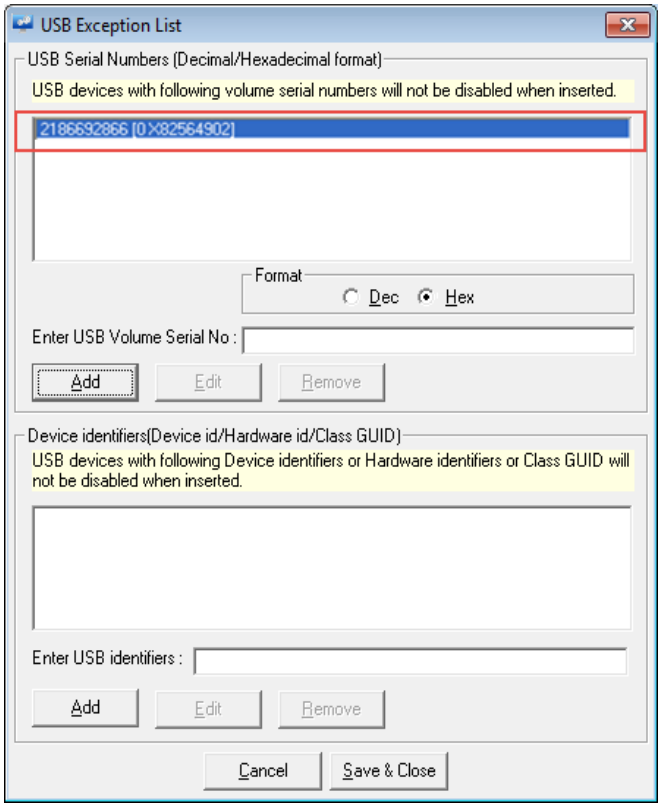


Figure 9

NOTE:

- In the command prompt, the volume serial number will always be in the 'Hexadecimal' format. You can convert it into a 'Decimal' format if required.
- It works only for Pen drive and no other Mass storage devices.

4.3 Converting USB Serial number format

You can convert the USB serial number from Hexadecimal to Decimal format, and vice versa.

1. Enter the USB serial format in **USB Volume Serial No** field.

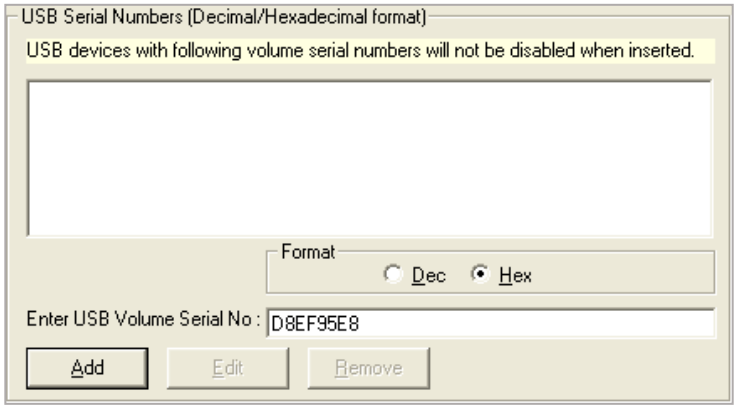


Figure 10

2. To convert the number in decimal format, click the **Dec** option.

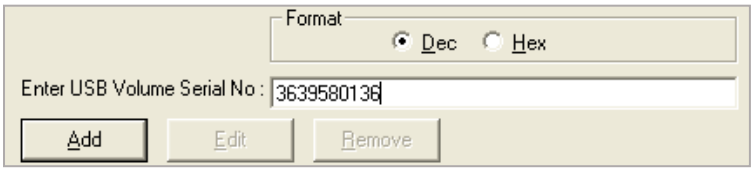


Figure 11

EventTracker automatically converts the number from Hexadecimal to Decimal.

3. To convert the number again in hexadecimal format, click the **Hex** option.

NOTE: EventTracker will not allow you to enter an invalid number (containing alphabet or signs) when the decimal (**Dec**) option is selected.

4.3.1 Device Identifiers (Device id/ Hardware id/ Class GUID)

The USB devices with the Device Identifiers- 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 the exception list:

1. Right click on Computer, select **Manage**.

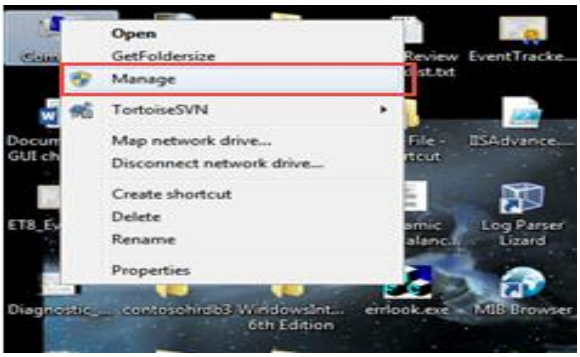


Figure 12

2. 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:

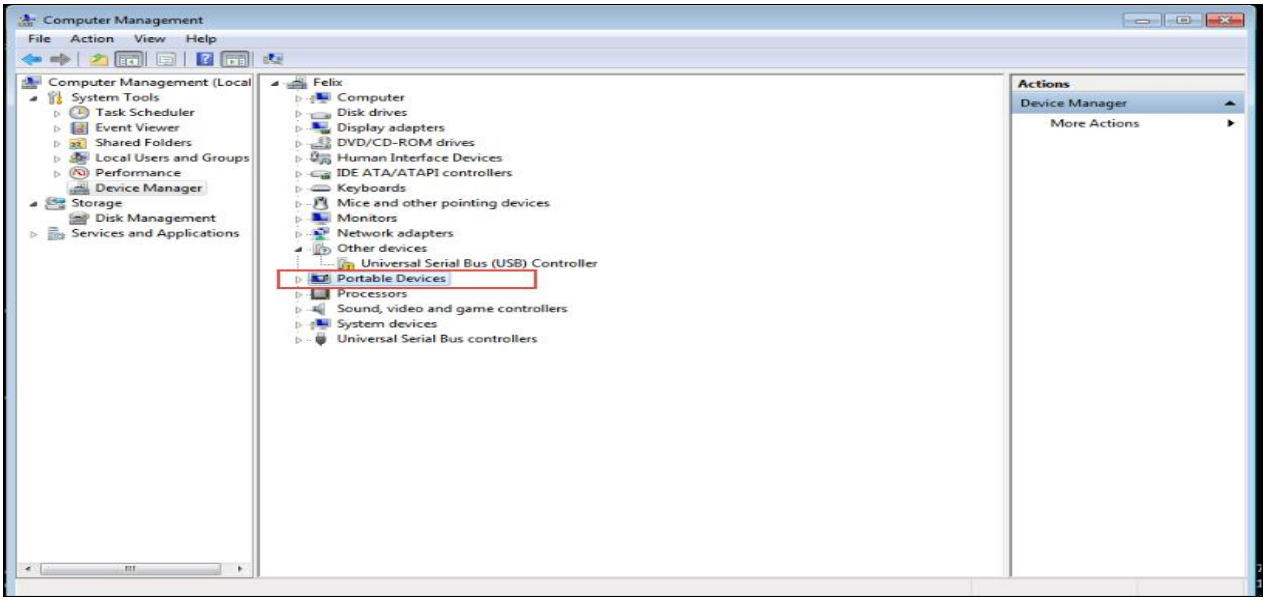


Figure 13

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.

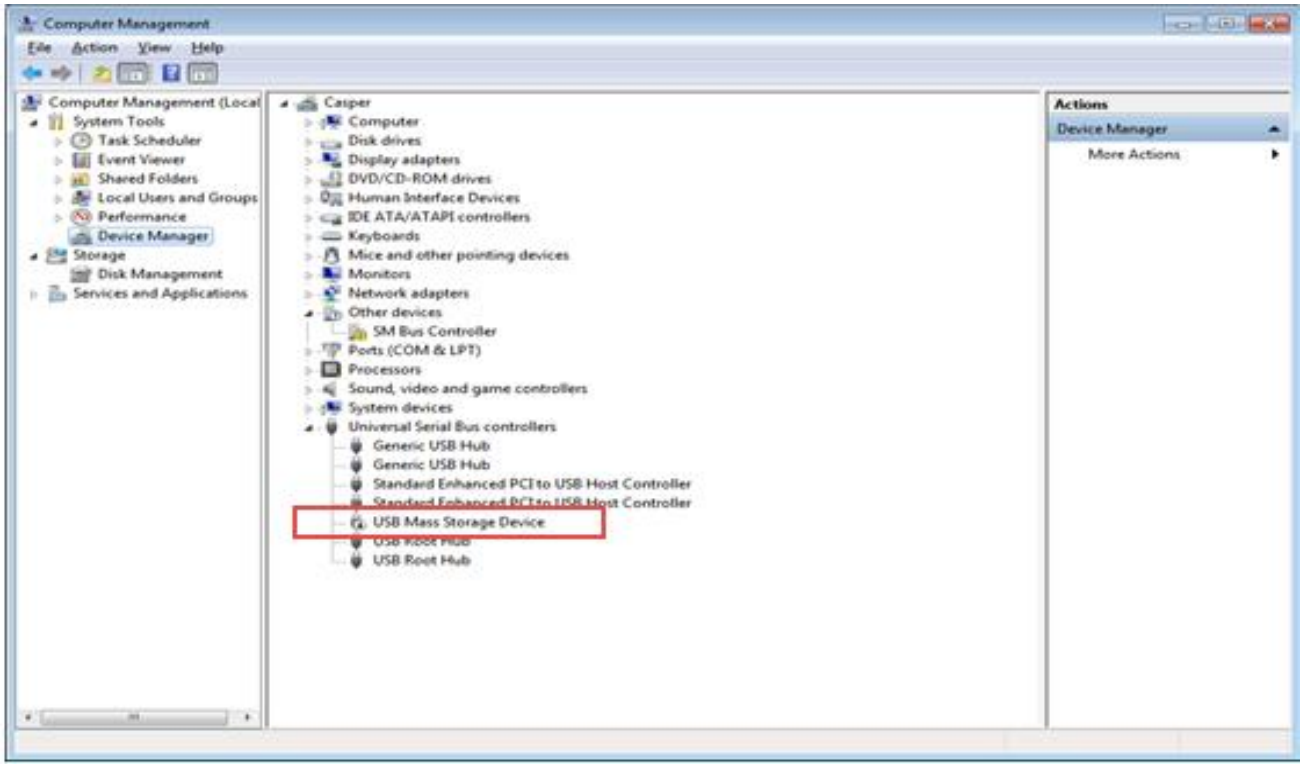


Figure 14

3. Right click on the **USB Mass Storage device**. Select **Properties**.

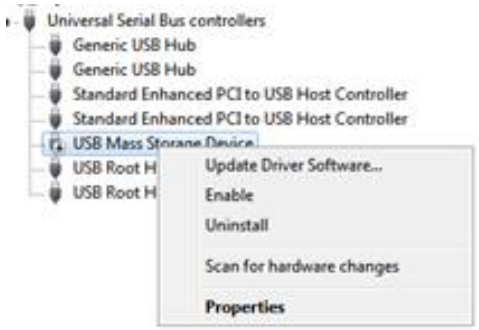


Figure 15

The USB Mass Storage Device Properties display.

1. Select the **Detail** tab.
2. In the **Property** option, select **Device Instance Path** from the dropdown list.

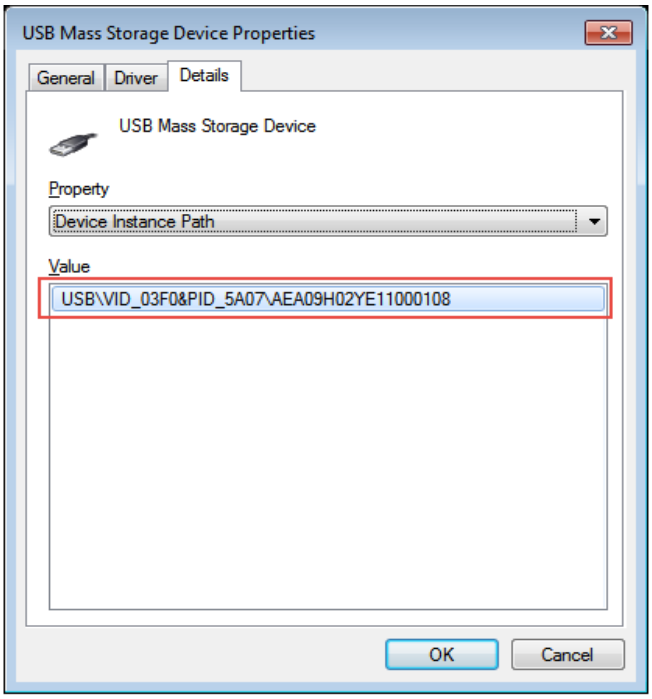


Figure 16

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

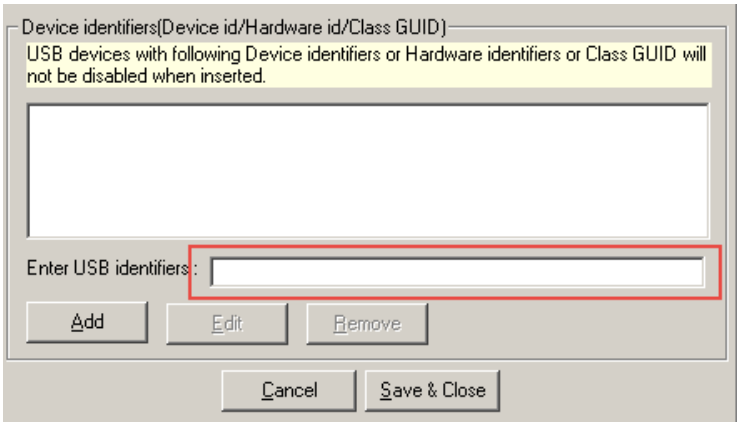


Figure 17

4. Click the **Add** button.

It gets added and is displayed.

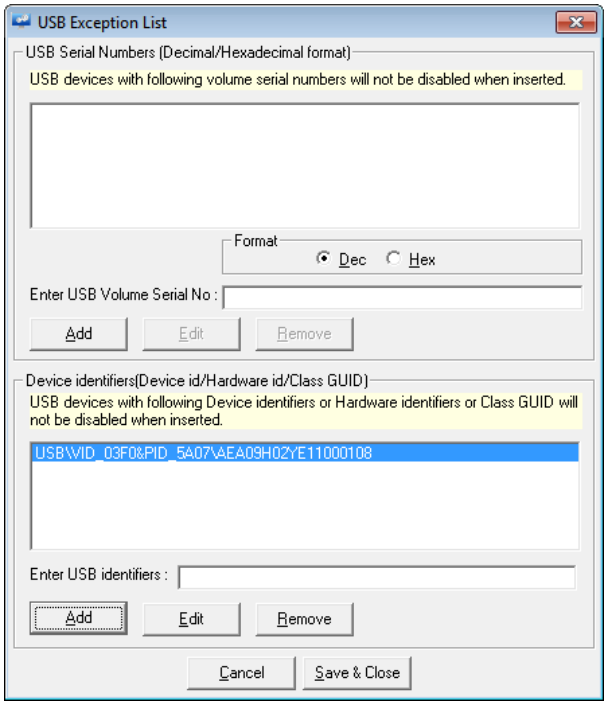


Figure 18

4.3.2 Possible Substring match for Device ID

The **Disable USB Devices** checkbox when clicked blocks the entry of all the USB devices. However, for the authentic USB devices, we can add its USB serial number or device ID to allow the USB data transfer.

The following are the possible substring match for the **Device ID** to allow more than one device at a time.

1. **To allow devices from a particular vendor:** Enter only the VID part like USB\Vid_0781
   In this example, 0781 is for SanDisk.

2. **To allow devices from a particular vendor and a particular product:**
   Enter VID and PID parts like USB\Vid_0781&Pid_5567
   In this example, 5567 is for SanDisk Cruzer Blade.

3. **To allow a device from a particular vendor and a particular product:**

   Enter VID, PID, and device serial number like
   USB\Vid_0781&Pid_5567\20040203321B6B6256E9

   Click here for more details on PID/VID.

b) Hardware id: Remains the same for a 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)

1. For adding Hardware id to the exception list,
2. Select **Hardware id** from the dropdown list in the **Property** option.

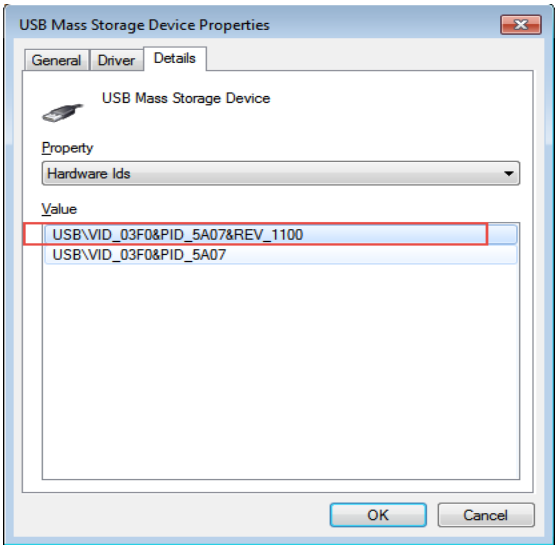


Figure 19

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

It gets added and displayed.

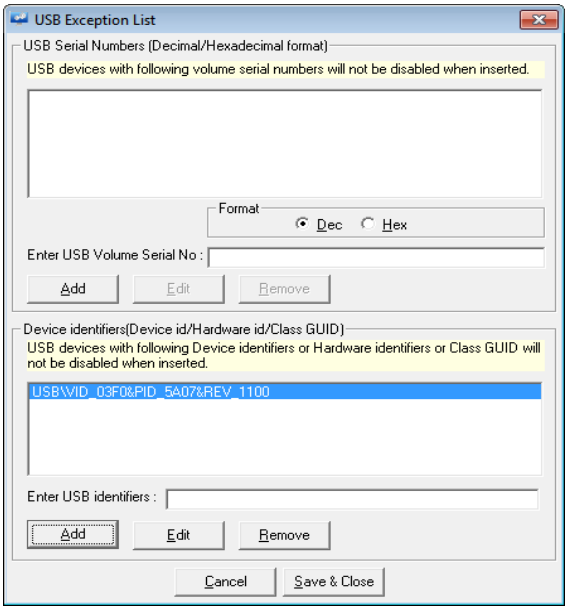


Figure 20

c) **Class GUID**: Remains the same for a device class.(e.g. class GUID of the optical mouse will be the 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}
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}

Devices	Value
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 the exception list,

1. Select Device Class GUID from the dropdown list.

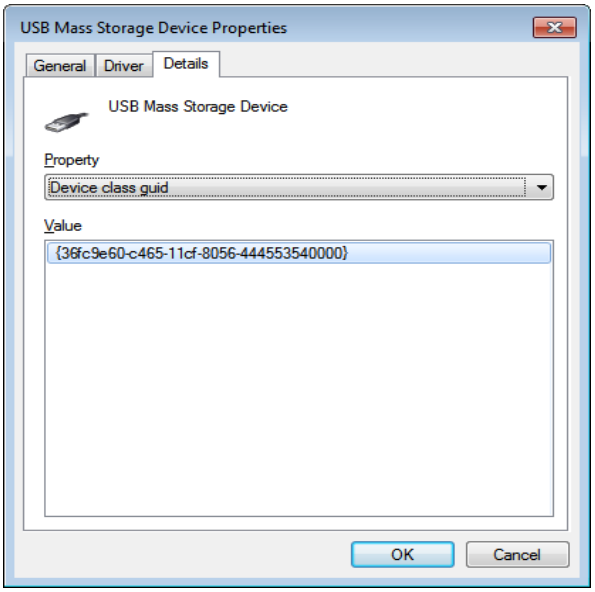


Figure 21

2. Copy and paste and the Value: in the **Device Identifier** field.
3. Click the **Add** button.

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

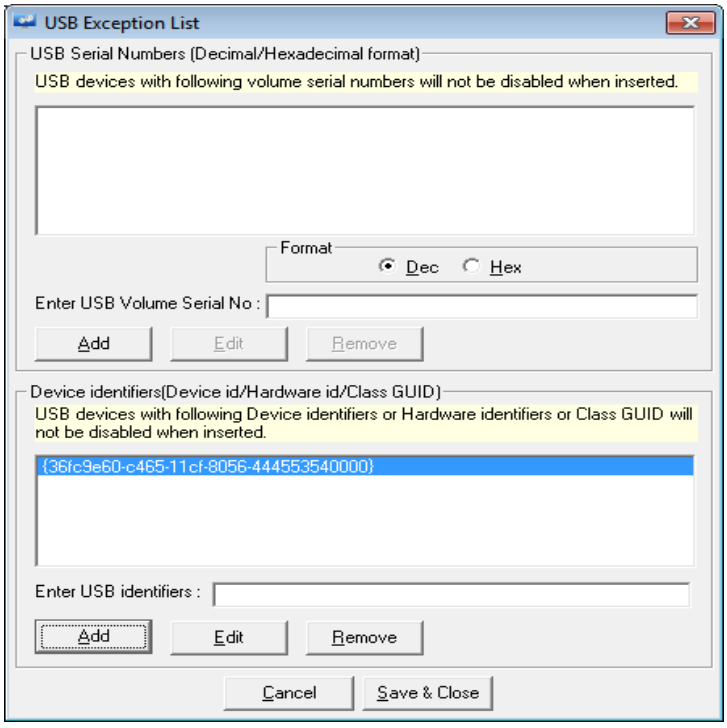


Figure 22

4. Click **Save & Close**.
5. Click **Save** on the System Monitoring page.

4.4 Configure Device Monitoring Alerts

Configure Alerts to receive notifications. You can also view these Alert events on the Alerts Dashboard.

4.4.1 Configure USB Device Monitor Alerts

1. Click the **Admin** drop-down list and then click **Alerts**.
2. Locate the **EventTracker: USB device disabled** & **Media Insert Alerts**.
3. Select the severity of the threat from the **Threat Level** drop-down list.
4. Select the check box under **Active**, if not selected.
5. Set appropriate Alert actions to receive notifications.
6. Click **OK** on the message box.

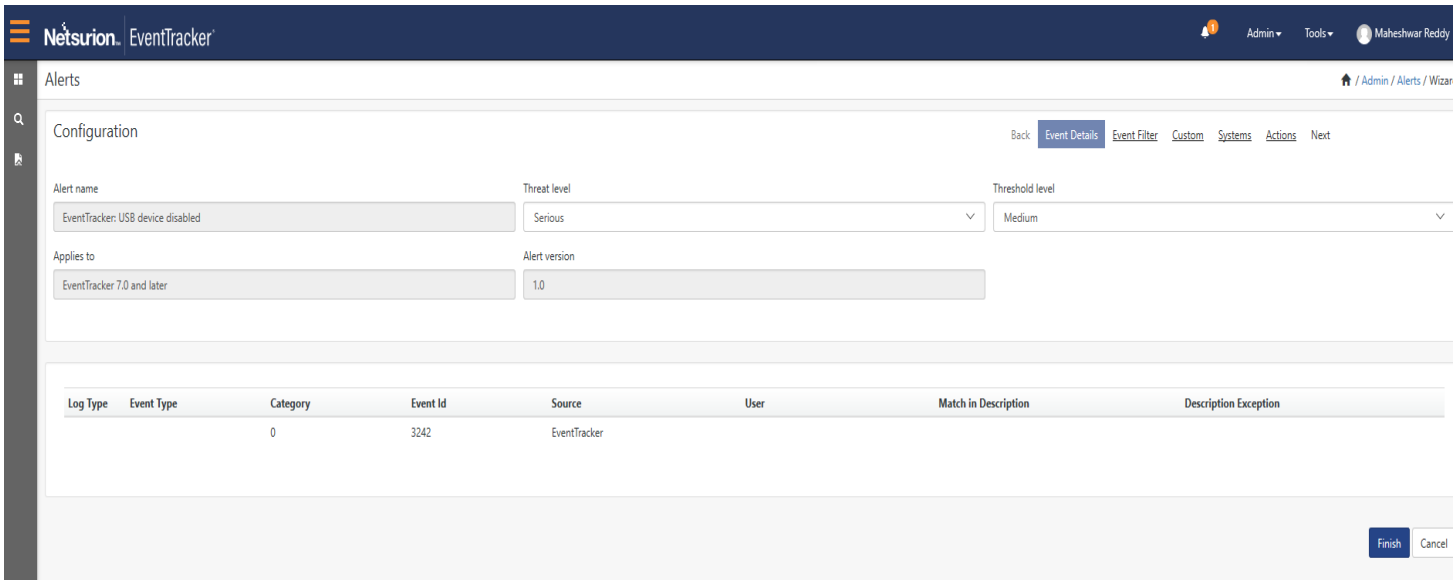


Figure 23

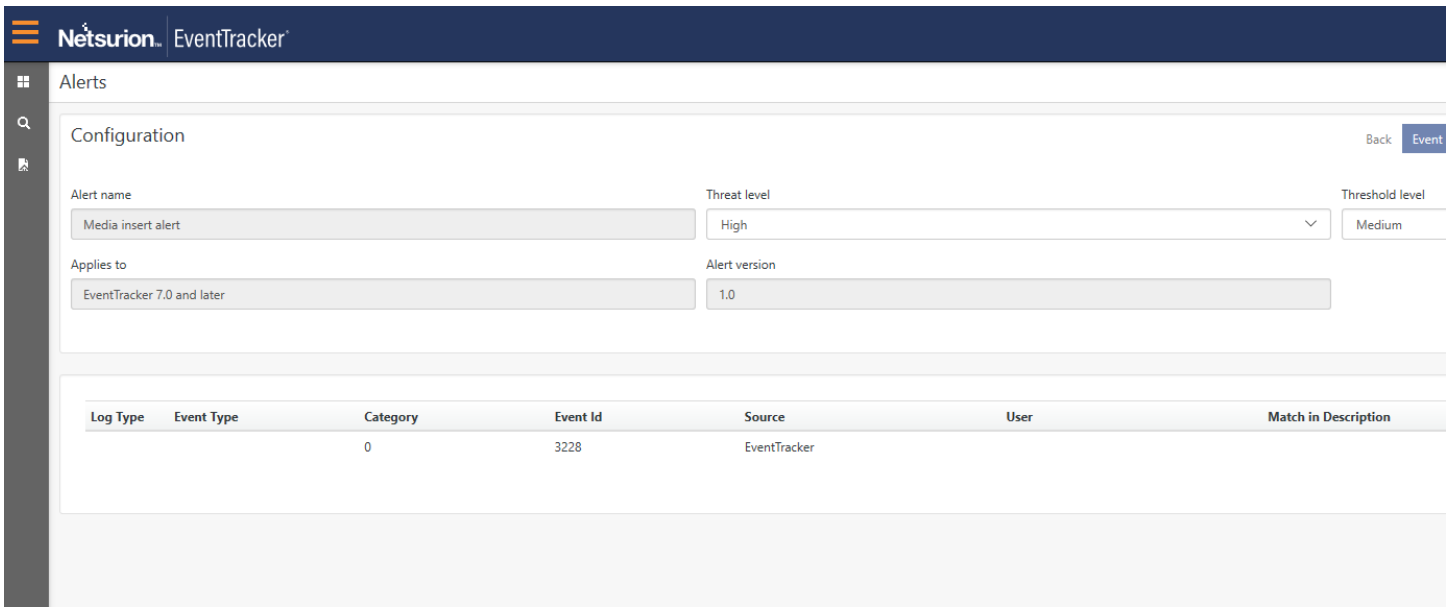


Figure 24

4.5 EventTracker Device Monitoring Categories

To view Categories, click the **Admin** drop-down list and then click **Category**.

Category: EventTracker: USB device disabled

Description: All events logged by EventTracker when it disables the unauthorized USB devices, which is not in the exception list. Event Id: 3242.

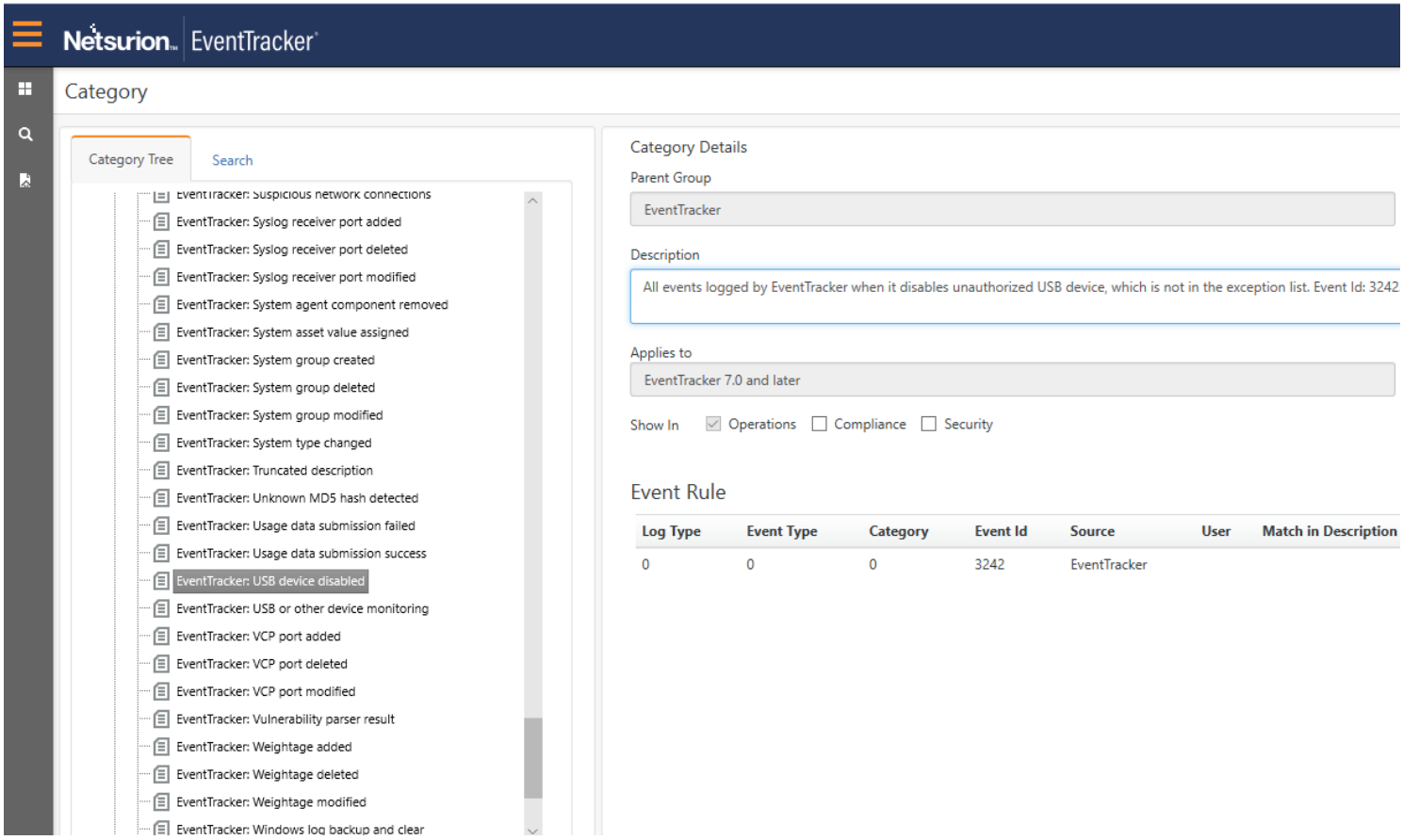


Figure 25

Category: EventTracker: USB or other device monitoring

Description: All events logged by EventTracker while monitoring USB, CD, and DVD device or media insertion and removal. Event Id: 3228, 3229, 3239, 3240.

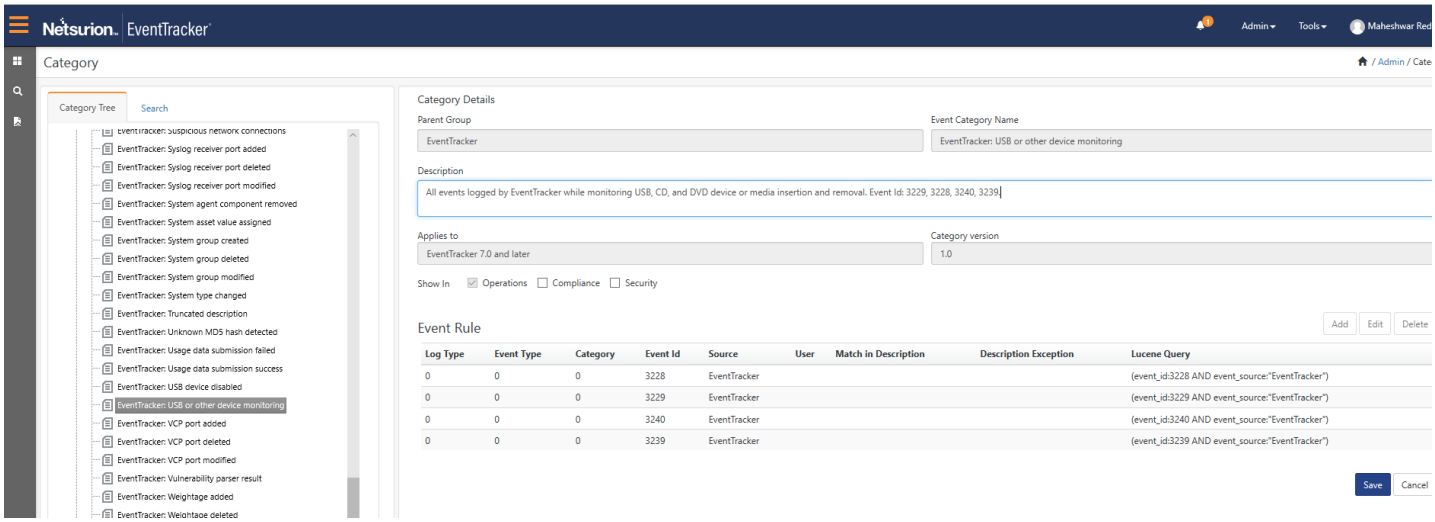


Figure 26

4.6 EventTracker Device Monitoring Reports

Operations -> Reports -> EventTracker: USB or other device monitoring

EventTracker Agent for Windows can be configured to monitor insert/removal and files added/modified/deleted/copied to and from removable media. If this feature is enabled, this report provides information on those activities across selected computers for the chosen time period.

Usage: This report must be run and reviewed regularly for all critical servers and workstations.

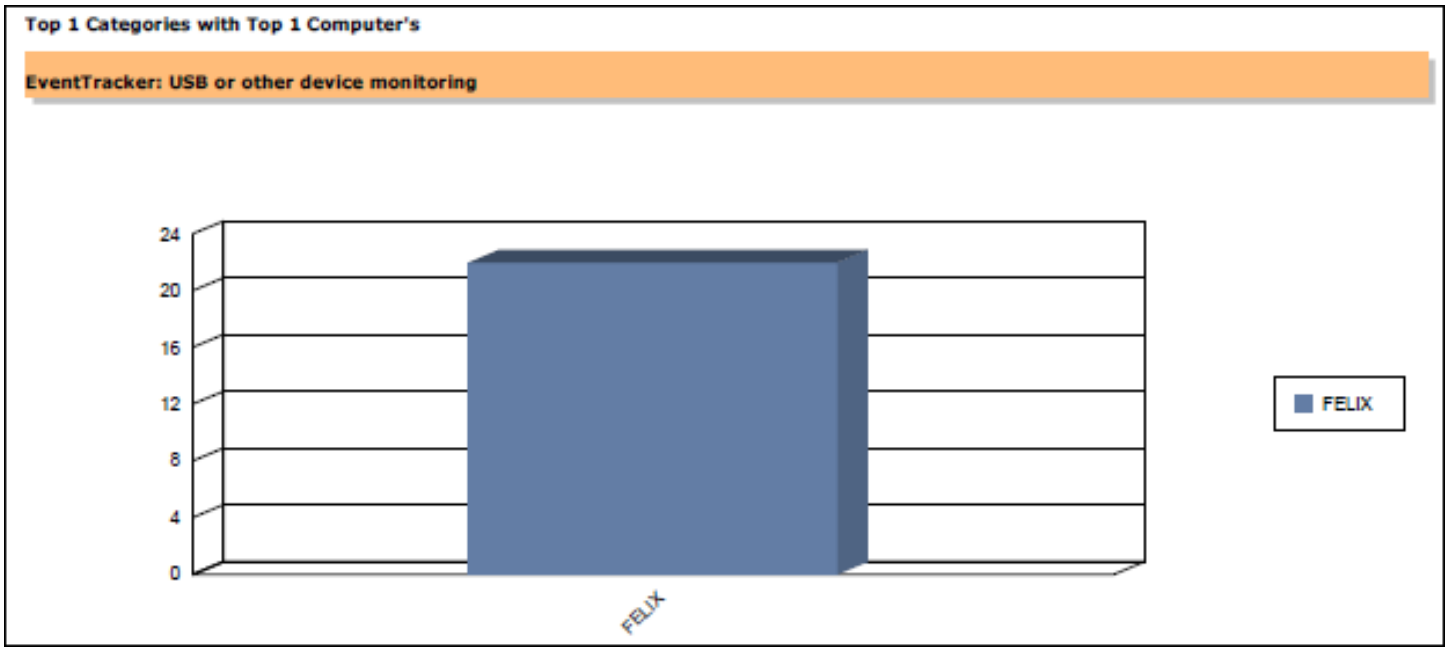


Figure 27

Category Detail Report Sorted By Computer

Category EventTracker: USB or other device monitoring had 1 Computers generating 22 events

Event IDs included are 3228, 3229, 3239, 3240

Computer FELIX generated 22 events. Details of Events are given below.

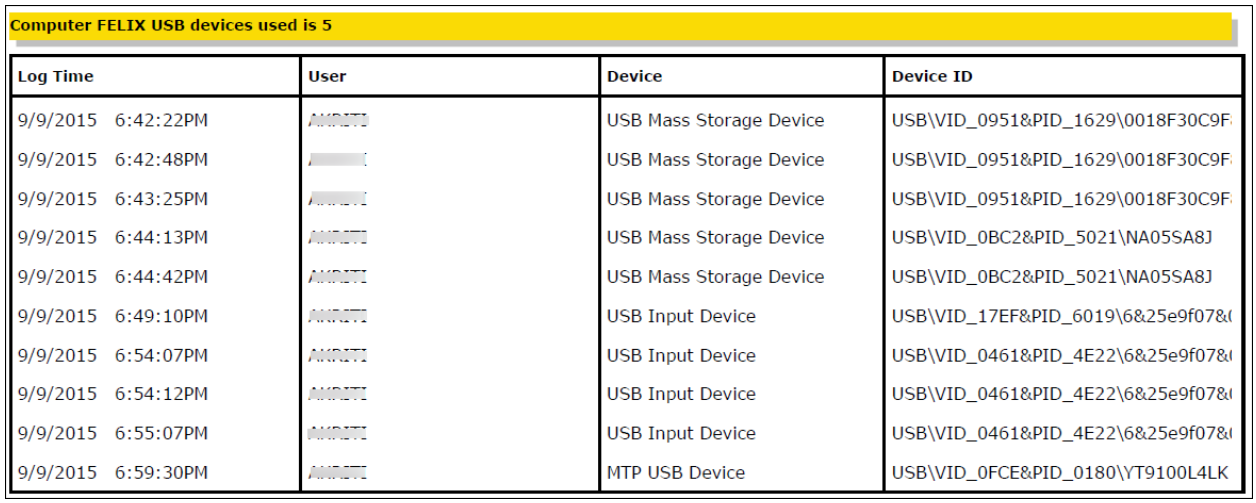
Log Time	User	Event Id	Source	Event Description
9/7/2015 3:12:57 PM		3228	EventTracker	Detected new drive <F:> Device Type: Fixed Volume Label: FreeAgent GoFlex Drive Volume Serial No: 1546817573 Volume ID: \\?\Volume{8c5f0eaa-f5d0-11e4-bf06-fcf286e6e67f}\ File System: NTFS Device ID: USB\VID_0BC2&PID_5021\NA05SA8J Network Volume: No Description: Change affects physical device or drive. <EventData><Data>Detected new drive <F:> Device Type: Fixed Volume Label: FreeAgent GoFlex Drive Volume Serial No: 1546817573 Volume ID: \\?\Volume{8c5f0eaa-f5d0-11e4-bf06-fcf286e6e67f}\ File System: NTFS Device ID: USB\VID_0BC2&PID_5021\NA05SA8J Network Volume: No Description: Change affects physical device or drive.</Data></EventData>
9/7/2015 3:14:45 PM		3229	EventTracker	Drive <F:> removed. Network Volume: No Description: Change affects physical device or drive. <EventData><Data>Drive <F:> removed. Network Volume: No Description: Change affects physical device or drive.</Data></EventData>

Figure 28

Operations -> Reports -> USB Device Disabled Report

This report provides information on the disabled USB devices across selected computers for the chosen time period.

Usage: This report would be useful when you are looking for a quick report on disabled USB devices.



Computer FELIX USB devices used is 5

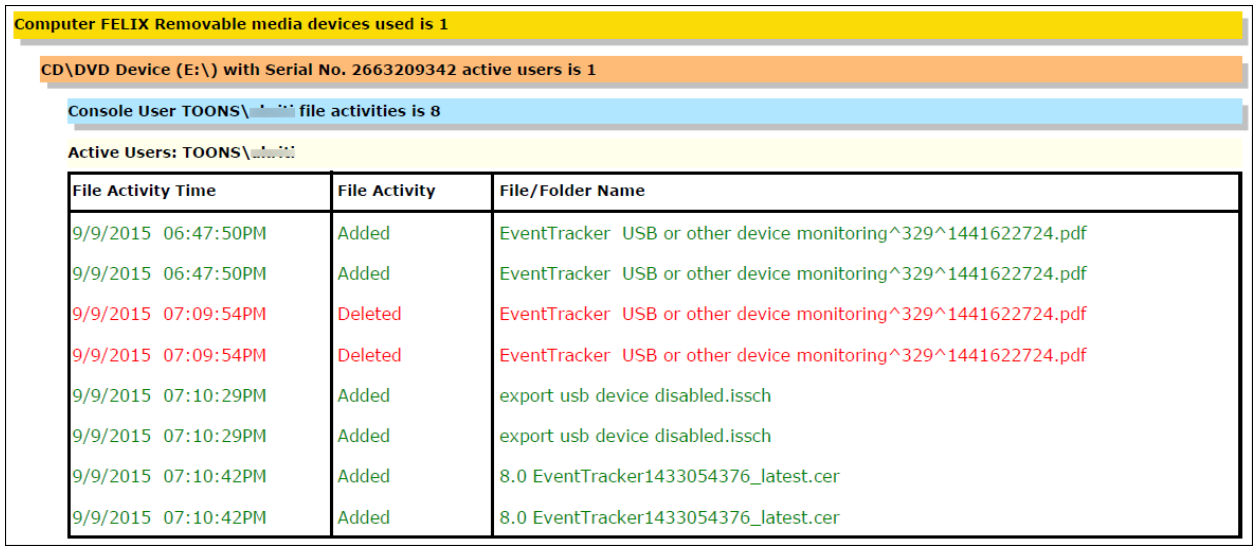
Log Time	User	Device	Device ID
9/9/2015 6:42:22PM	[redacted]	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:42:48PM	[redacted]	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:43:25PM	[redacted]	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:44:13PM	[redacted]	USB Mass Storage Device	USB\VID_0BC2&PID_5021\NA05SA8J
9/9/2015 6:44:42PM	[redacted]	USB Mass Storage Device	USB\VID_0BC2&PID_5021\NA05SA8J
9/9/2015 6:49:10PM	[redacted]	USB Input Device	USB\VID_17EF&PID_6019\6&25e9f07&(
9/9/2015 6:54:07PM	[redacted]	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:54:12PM	[redacted]	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:55:07PM	[redacted]	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:59:30PM	[redacted]	MTP USB Device	USB\VID_0FCE&PID_0180\YT9100L4LK

Figure 29

Operations -> Reports -> USB Device Report -> USB Device Report Detail

This report provides detailed information on the files added/modified/deleted to the USB device. It can be tuned by applying Refine or Filter criteria, systems, and time period.

Usage: This report is usually run during a detailed investigation phase, as needed.



Computer FELIX Removable media devices used is 1

CD\DVD Device (E:\) with Serial No. 2663209342 active users is 1

Console User TOONS\[redacted] file activities is 8

Active Users: TOONS\[redacted]

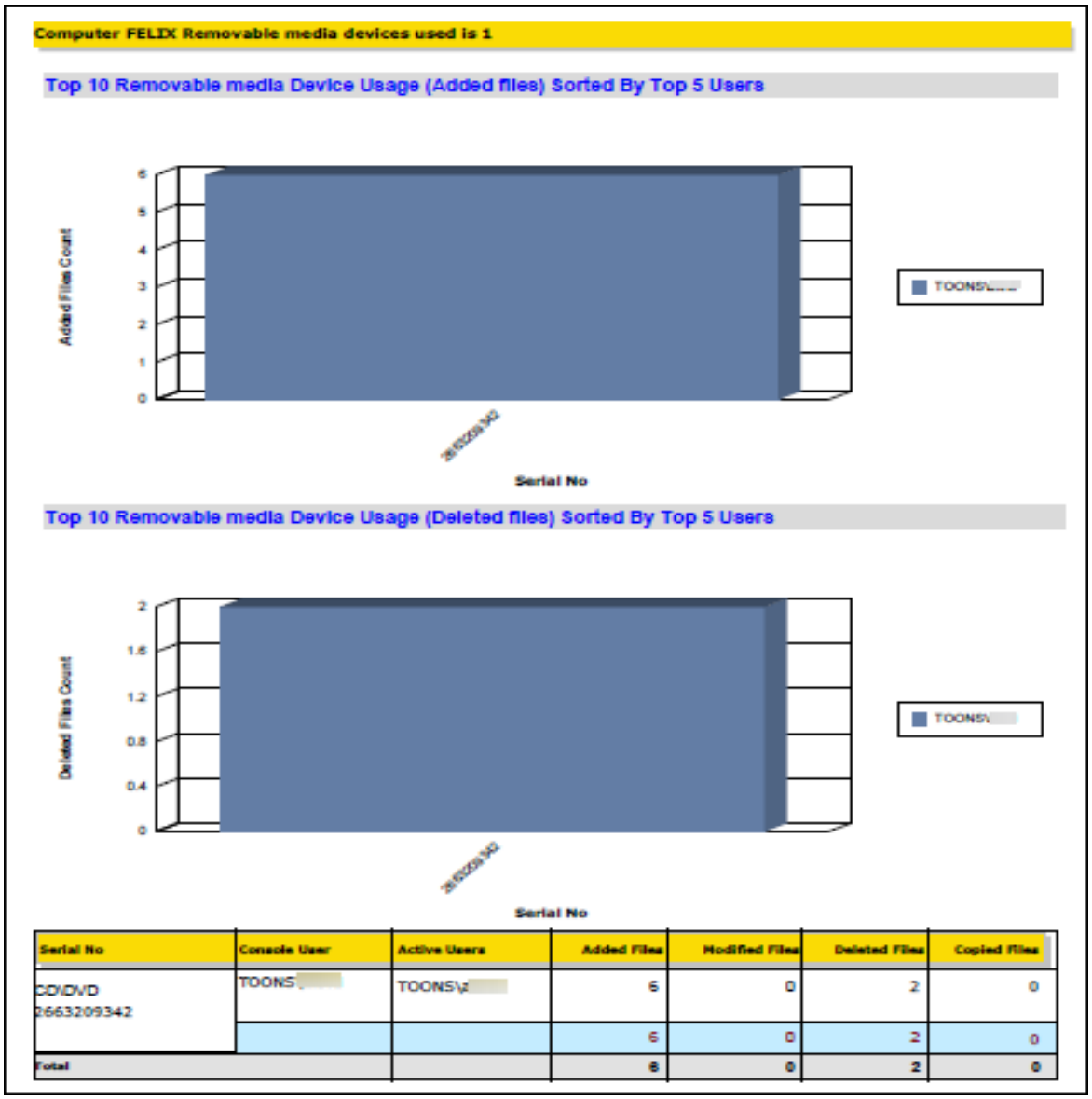
File Activity Time	File Activity	File/Folder Name
9/9/2015 06:47:50PM	Added	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 06:47:50PM	Added	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 07:09:54PM	Deleted	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 07:09:54PM	Deleted	EventTracker USB or other device monitoring^329^1441622724.pdf
9/9/2015 07:10:29PM	Added	export usb device disabled.issch
9/9/2015 07:10:29PM	Added	export usb device disabled.issch
9/9/2015 07:10:42PM	Added	8.0 EventTracker1433054376_latest.cer
9/9/2015 07:10:42PM	Added	8.0 EventTracker1433054376_latest.cer

Figure 30

Operations -> Reports -> USB Device Report -> USB Device Report Summary

This report provides summary information on the files added/modified/deleted to the USB device. Charts are included per system per activity top 10 USB devices sorted by the top 5 users.

Usage: This report would be useful when you are looking for a quick report for the files added/modified/deleted/copied to and from USB devices.



Serial No	Console User	Active Users	Added Files	Modified Files	Deleted Files	Copied Files
CD/DVD 2663209342	TOONS	TOONS\z	6	0	2	0
			6	0	2	0
Total			6	0	2	0

Figure 31

4.7 EventTracker Generated Events

EventTracker detected the new drive [3228]

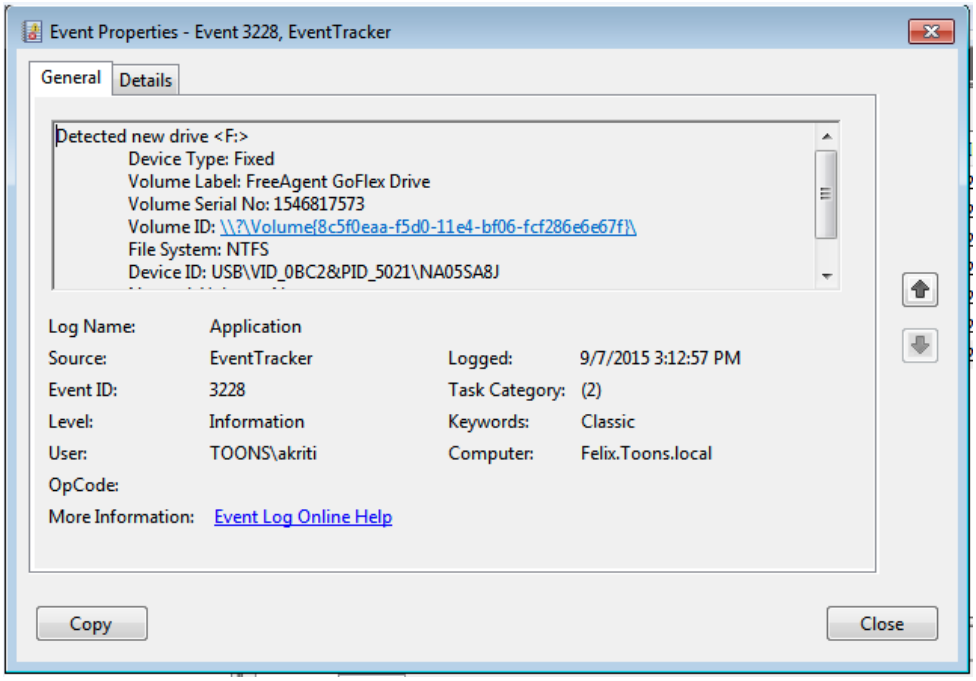


Figure 32

Description:

Detected new drive <F:>

Device Type: Fixed

Volume Label: FreeAgent GoFlex Drive

Volume Serial No: 1546817573

Volume ID: \\?\Volume{8c5f0eaa-f5d0-11e4-bf06-fcf286e6e67f}\

File System: NTFS

Device ID: USB\VID_0BC2&PID_5021\NA05SA8J

Network Volume: No

Description: Change affects physical devices or drive.

EventTracker <drive name> removed [3229]

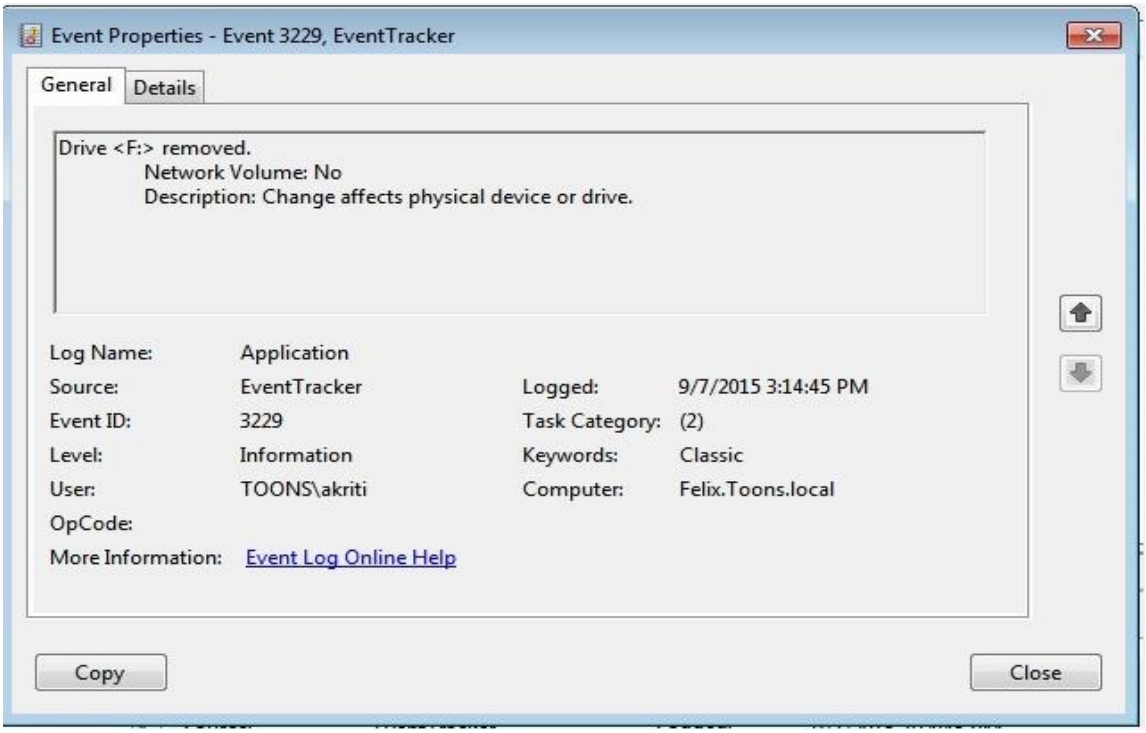


Figure 33

Description:

Drive <F:> removed.

Network Volume: No

Description: Change affects physical device or drive.

USB device is disabled by EventTracker [3242]

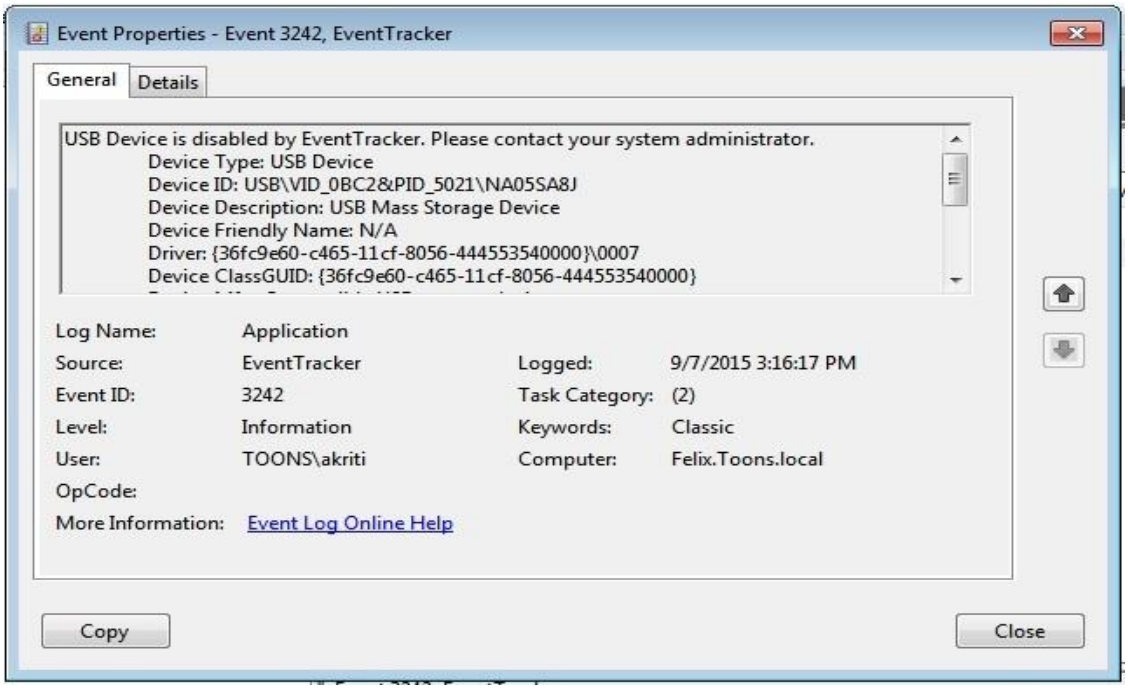


Figure 34

Description:

USB Device is disabled by EventTracker. Please contact your system administrator.

Device Type: USB Device

Device ID: USB\VID_0BC2&PID_5021\NA05SA8J

Device Description: USB Mass Storage Device

Device Friendly Name: N/A

Driver: {36fc9e60-c465-11cf-8056-444553540000}\0007

Device ClassGUID: {36fc9e60-c465-11cf-8056-444553540000}

Device Mfg: Compatible USB storage device

Hardware ID: USB\VID_0BC2&PID_5021&REV_0148

Enumerator: USB

Local Information: Port_#0002.Hub_#0003

Physical Device Object Name: \Device\USBPDO-6

Service Name: USBSTOR

BUS Number: 0

Capability: Removable UniqueID RawDeviceOK SurpriseRemovalOK

USB Monitoring started for<drive name> [3239]

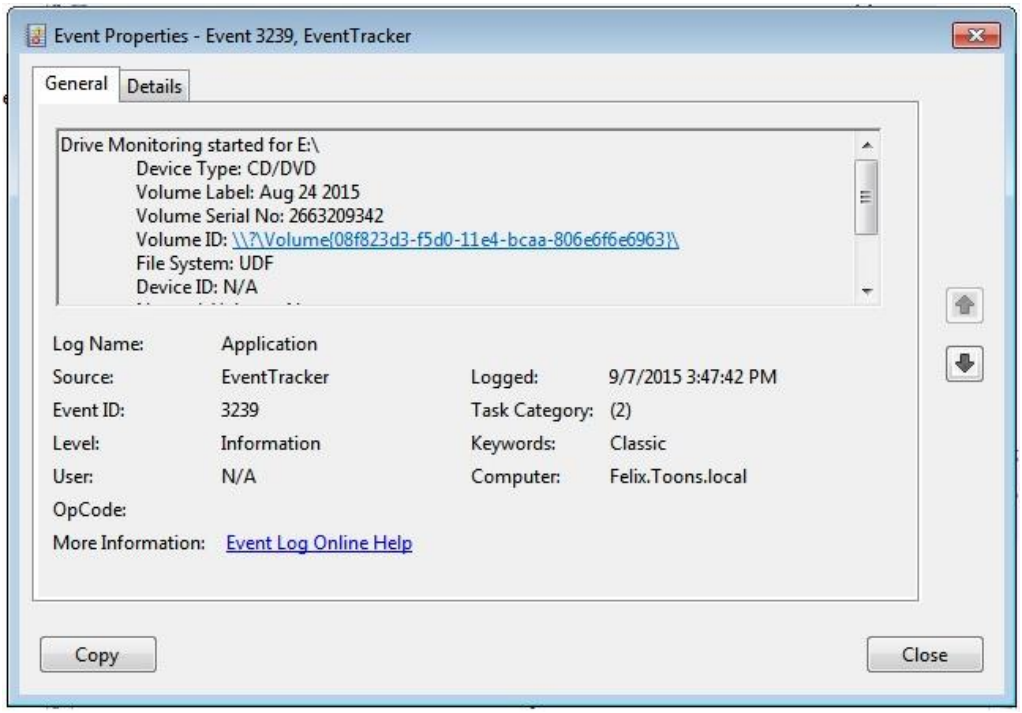


Figure 35

Description:

Drive Monitoring started for E:\

Device Type: CD/DVD

Volume Label: Aug 24 2015

Volume Serial No: 2663209342

Volume ID: \\?\Volume{08f823d3-f5d0-11e4-bcaa-806e6f6e6963}\

File System: UDF

Device ID: N/A

Network Volume: No

Description: Change affects media in drive.

Console User: TOONS\akriti

Active Users: TOONS\akriti

USB Monitoring stopped for<drive name> [3240]

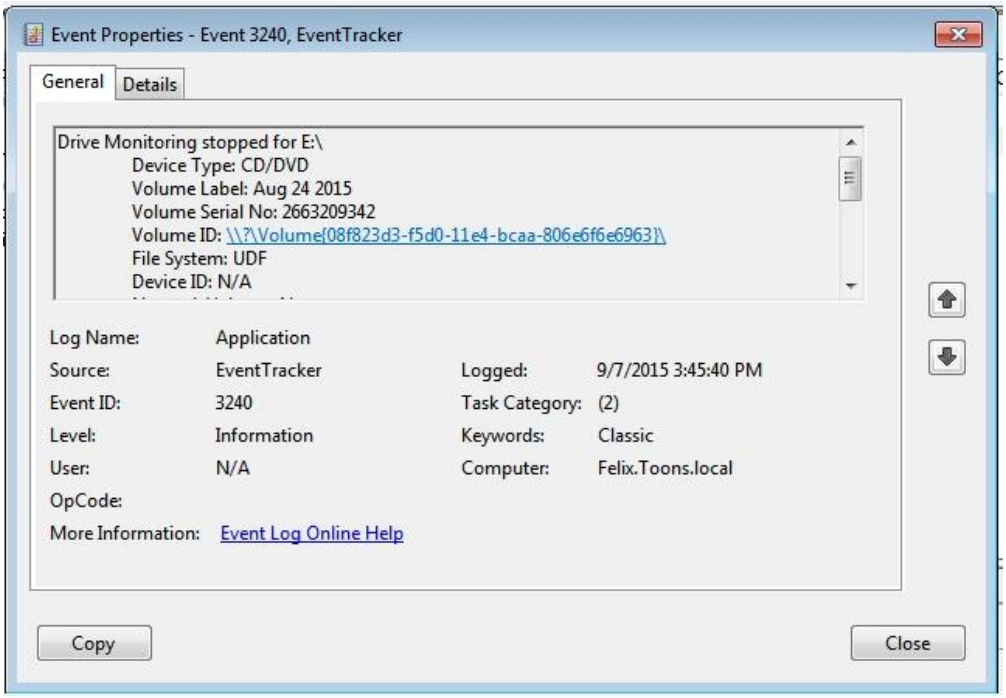


Figure 36

Description:

Drive Monitoring stopped for E:\

Device Type: CD/DVD

Volume Label: Aug 24 2015

Volume Serial No: 2663209342

Volume ID: \\?\Volume{08f823d3-f5d0-11e4-bcaa-806e6f6e6963}\

File System: UDF

Device ID: N/A

Network Volume: No

Description: Change affects media in drive.

Console User: TOONS\akriti

Active Users: TOONS\akriti

Files copied by using Live File System:

USBDeview|Added|09/07/2015 03:44:46 PM

Files accessed by user: TOONS\akriti

desktop.ini|Existing|09/07/2015 02:23:19 PM

4.8 Limitations

EventTracker Windows Agent monitors CD/DVD burning activities carried only through the Windows Explorer and does not monitor burning activities done via third party tools such as Nero, Iomega, etc.