Abstract

With the introduction of newer portable devices, the security needs of protecting integrity and confidential data has been changed. An increasing need of portable access to the data has also increased the risk of sensitive or confidential data exposure. Therefore, to keep a record of removable media device activities has become one of the most important compliance factors for the enterprise. EventTracker's advanced removable media monitoring capacity protects and monitors system(s) from illegal access or data theft. EventTracker helps user(s) to disable the unauthorized access to the machine and allow the trusted devices connection.

Purpose

This document will help you to enable the removable device monitoring and explains the procedure to find the Device ID and USB serial number. It also monitors insertion/removal and files written to and read from removable media such as CD/DVD and USB.

Intended Audience

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

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8. The instructions can be used while working with later releases of EventTracker Enterprise.
# Table of Contents

Overview ....................................................................................................................................................... 3
EventTracker Monitoring Features ............................................................................................................ 3
Implement Monitoring Removable Media Feature in EventTracker v8 ................................................. 5
  Monitor CDW / DVD Burning Activities ................................................................................................. 6
  Monitor CD-ROM Activities .................................................................................................................. 6
  Configure EventTracker Agent to Monitor Removable Media ............................................................ 6
Exempt Authorized USB Drives .................................................................................................................. 9
  USB Volume serial Number ................................................................................................................... 9
  To find USB volume serial number .................................................................................................... 10
  To convert USB Serial number format .............................................................................................. 12
    Device Identifiers (Device id / Hardware id / Class GUID) .............................................................. 13
    Possible Substring match for Device ID .......................................................................................... 18
Configure Device Monitoring Alerts ...................................................................................................... 25
  Configure USB Device Monitor Alerts .............................................................................................. 25
EventTracker Device Monitoring Categories ........................................................................................... 26
EventTracker Device Monitoring Reports ............................................................................................... 27
EventTracker Generated Events ........................................................................................................... 32
Limitations ............................................................................................................................................. 37
Overview

The USB and removable media are vital part of any enterprise when it comes to data transfer. They have many shapes as flash memory drives, cell phones, cameras, and PDAs that can serve as storage devices. These portable devices are convenient for transfer and storage of large data with or without network access and that too in short time. However, with all these advantages, it has some security vulnerabilities. In 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 has also increased.

As a SIEM solution, EventTracker not only has the ability to 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 system.

EventTracker Monitoring Features

Reports insertion / removal of the removable device

EventTracker will log every activity of the USB or other removable media device like 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.

Prevents unauthorized access and reports the intrusion in real time

Every time an USB is inserted, the EventTracker agent looks at 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.

Restricts Access

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

**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.

**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.

![Alert Configuration](image)

**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 Enterprise** >> Click **Reports** menu >> Click **Dashboard** dropdown option >> Click the **Operations** tab. In the **Report Tree**, click **USB Device Report** node.
Implement Monitoring Removable Media Feature in EventTracker v8

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 USB device is unplugged or media is ejected, Windows sends media removal notification to the `USBTracker.exe`.
5. Upon receiving the notification, `USBTracker.exe` stops monitoring, generates event 3240 with details on all activities and exits.

NOTE:
This feature is supported for Windows only (Win XP, Vista, 2K3, and 2K8, 2K 12, Win 7, Win 8 and Win 8.1) and requires EventTracker Agent to be installed and configured.

Monitor CDW/DVD Burning Activities

Windows XP, 2003, 2008, 2012, Vista, Win7, Win 8 or Win 8.1 has 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 ‘staging area’. 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?

Monitor 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.

Configure EventTracker Agent to Monitor Removable Media

1. Click the Admin drop-down list and then click Windows Agent Config.
2. Select the system from the Select system drop-down list.
3. Click the System Monitor tab.
Report insert / remove check box is selected by default. Leave as it is.

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.
• **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.*

**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**

**USB AND OTHER DEVICE CHANGES**
- Report insert/remove
  - Record activity
- Disable USB devices
  - Mass Storage Devices
  - All Devices
  - All Devices (Except Human Interface Devices Class)

**USB EXCEPTION LIST**

**Figure 5**

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. Click **Save**.

**Exempt Authorized USB Drives**

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

1. Click **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:

**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.
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.
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.
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.

To convert 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.

   ![USB Serial number - Hexadecimal format](image)

   *Figure 9: USB Serial number - Hexadecimal format*

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

   ![USB Serial number - Decimal format](image)

   *Figure 10: USB Serial number - Decimal format*

   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 decimal (**Dec**) option is selected.

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 exception list:

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

![Figure 11](image)

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

![Figure 14](image1.png)

The USB Mass Storage Device Properties display.

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

![Figure 15](image2.png)
- Copy the **Value** highlighted in the figure above and paste it in the **Device Identifiers** field as displayed in the figure below:

![Device Identifiers](image)

- Click the **Add** button.

It gets added and is displayed.
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.

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

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

- **To allow a particular 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 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.
• Copy the value and paste it in the **Device identifiers** field.
• Click the **Add** button.

It gets added and displayed.

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.
<table>
<thead>
<tr>
<th>Devices</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery</td>
<td>{72631e54-78a4-11d0-bcf7-00aa00b7b32a}</td>
</tr>
<tr>
<td>Biometric</td>
<td>{53D29EF7-377C-4D14-B64B-EB3AB5769359}</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>{e0c9f06c-cd8b-4647-bb8a-263b43f0f974}</td>
</tr>
<tr>
<td>CDROM</td>
<td>{4d36e965-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>DiskDrive</td>
<td>{4d36e967-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Display</td>
<td>{4d36e968-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>FDC</td>
<td>{4d36e969-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>FloppyDisk</td>
<td>{4d36e980-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>HDC</td>
<td>{4d36e96a-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>HIDClass</td>
<td>{745a17a0-74d3-11d0-b6fe-00a0c90f57da}</td>
</tr>
<tr>
<td>Dot4</td>
<td>{48721b56-6795-11d2-b1a8-0080c72e74a2}</td>
</tr>
<tr>
<td>Dot4Print</td>
<td>{49cf6ac8-6f86-11d2-b1e5-0080c72e74a2}</td>
</tr>
<tr>
<td>61883</td>
<td>{7ebebf0c-3200-11d2-b4c2-00a0c9697d07}</td>
</tr>
<tr>
<td>AVC</td>
<td>{c06ff265-ae09-48f0-b12c-16753d7cba83}</td>
</tr>
<tr>
<td>SBP2</td>
<td>{4e8179be-ec20-11d1-b6b8-00c04fa372a7}</td>
</tr>
<tr>
<td>1394</td>
<td>{6bd1f1c1-810f-11d0-bec7-08002be2092f}</td>
</tr>
<tr>
<td>Image</td>
<td>{6bd1f1c6-810f-11d0-bec7-08002be2092f}</td>
</tr>
<tr>
<td>Infrared</td>
<td>{6bd1f1c5-810f-11d0-bec7-08002be2092f}</td>
</tr>
<tr>
<td>Keyboard</td>
<td>{4d36e96b-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>MediumChanger</td>
<td>{ce5939ae-ebde-11d0-b181-0000f8753ec4}</td>
</tr>
<tr>
<td>MTD</td>
<td>{4d36e970-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Modem</td>
<td>{4d36e96d-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Monitor</td>
<td>{4d36e96e-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Mouse</td>
<td>{4d36e96f-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Multifunction</td>
<td>{4d36e971-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Media</td>
<td>{4d36e96c-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>MultiportSerial</td>
<td>{50906cb8-ba12-11d1-bf5d-0000f805f530}</td>
</tr>
<tr>
<td>Net</td>
<td>{4d36e972-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>NetClient</td>
<td>{4d36e973-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>NetService</td>
<td>{4d36e974-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>NetTrans</td>
<td>{4d36e975-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>SecurityAccelerator</td>
<td>{268c95a1-edfe-11d3-95c3-0010dc405a05}</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>{4d36e977-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Ports</td>
<td>{4d36e978-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Printer</td>
<td>{4d36e979-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Processor</td>
<td>{50127dc3-0f36-415e-a6cc-4cb3be910b65}</td>
</tr>
<tr>
<td>SCSIAdapter</td>
<td>{4d36e9b7-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>Sensor</td>
<td>{5175d334-c371-4806-b3ba-71fd53c9258d}</td>
</tr>
<tr>
<td>SmartCardReader</td>
<td>{509d5230-ba8a-11d1-bf5d-0000f805f530}</td>
</tr>
<tr>
<td>Volume</td>
<td>{71a27cdd-812a-11d0-bec7-08002be2092f}</td>
</tr>
<tr>
<td>System</td>
<td>{4d36e97d-e325-11ce-bfc1-108002be1031}</td>
</tr>
<tr>
<td>TapeDrive</td>
<td>{6d807784-7d21-11cf-801c-08002be1031}</td>
</tr>
<tr>
<td>USB</td>
<td>{36fc9e60-c465-11cf-8056-444553540000}</td>
</tr>
</tbody>
</table>
### EventTracker: Removable Media Device Monitoring

<table>
<thead>
<tr>
<th>Devices</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows CE USB ActiveSync Devices (WCEUSBS)</td>
<td>{25dbce51-6c8f-4a72-8a6d-b54c2b4fc835}</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Device</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Portable Devices (WPD)</td>
<td>{ee5ad98-8080-425f-922a-dabf3de3f69a}</td>
</tr>
<tr>
<td>USB</td>
<td>{36fc9e60-c465-11cf-8056-444553540000}</td>
</tr>
</tbody>
</table>


For adding Class GUID in exception list,

- Select Device Class GUID from the dropdown list.
• 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:
4. Click **Save & Close**.
5. Click **Save** on the System Monitoring page.
Configure Device Monitoring Alerts

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

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 severity of 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.
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 unauthorized USB device, which is not in the exception list. Event Id: 3242.

**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.
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 26
Operations -> Reports -> USB Device Disabled Report

This report provides information on disabled USB device 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.
Operations -> Reports -> USB Device Report -> USB Device Report Detail

This report provides detailed information on the files added/modified/deleted to 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.

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

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

![Figure 30](image-url)
EventTracker Generated Events

EventTracker detected new drive [3228]

![Event Properties - Event 3228, EventTracker](image)

Description:

Detected new drive <F:>

- **Device Type:** Fixed
- **Volume Label:** FreeAgent GoFlex Drive
- **Volume Serial No:** 1546817573
- **Volume ID:** `\Volume(8c5f0eaa-f5d0-11e4-bf06-fcfc86e6e67f)`
- **File System:** NTFS
- **Device ID:** `USB\VID_0BC2&PID_5021\NA05SA8J`

Figure 31
Network Volume: No
Description: Change affects physical device or drive.

**EventTracker <drive name> removed [3229]**

---

![Event Properties - Event 3229, EventTracker](image)

Log Name: Application
Source: EventTracker
Event ID: 3229
Level: Information
User: TOONS\akriti
OpCode: 
More Information: [Event Log Online Help](#)

Description:

Drive <F:> removed.
Network Volume: No
Description: Change affects physical device or drive.

---

**USB device is disabled by EventTracker [3242]**
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
EventTracker: Removable Media Device Monitoring

 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]

![Event Properties - Event 3239, EventTracker](image)

**Figure 34**

**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]
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}\n
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

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.