



How-To Guide

Monitor Removable Media Devices in Netsurion Open XDR

Publication Date March 25, 2024

© Copyright Netsurion. All Rights Reserved.



Abstract

This document provides instructions to enable the Removable Media Monitoring feature in Netsurion Open XDR. It also explains the procedure for monitoring the activities of various removable media.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The Configuration details in this guide are consistent with Netsurion Open XDR 9.x.

Audience

This guide is for the administrators responsible for monitoring and managing events in Netsurion Open XDR.



Table of Contents

1	Ove	rview4
2	Nets	surion Open XDR Monitoring Features4
	2.1	Reports Insertion/Removal of the Removable Devices
	2.2	Prevents Unauthorized Access and Reports the Intrusion in Real-time
	2.3	Restricts Access
	2.4	Protects the System from Malware
	2.5	Logging USB Device Communication
	2.6	Alert Notification
	2.7	Configures Media Insertion Report
3	Enal	bling Removable Media Monitoring Feature6
	3.1	Monitoring CDW/DVD Burning Activities
	3.2	Monitoring CD-ROM Activities
	3.3 3.3.1	Configuring Netsurion Open XDR Agent to Monitor Removable Media
	3.3.2	Disable USB Devices
4	Exer	mpt Authorized USB Drives9
	4.1	USB Volume Serial Number
	4.2	Finding USB Volume Serial Number9
	4.3 4.3.1	Converting USB Serial Number Format
	4.4 4.4.1	Configure Device Monitoring Alerts
	4.5	Netsurion Open XDR Device Monitoring Categories19
	4.6 4.6.1	Netsurion Open XDR Device Monitoring Reports 20 USB or Other Device Monitoring 20
	4.6.2	USB Device Disabled Report 22
	4.6.3	USB Device Report Details
	4.6.4	USB Device Report Summary 22
	4.7	Netsurion Open XDR Generated Events



1 Overview

The USB and removable media are a vital part of any enterprise for data transfer. They have many forms such 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. 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 illegal data transfer, etc have also increased.

As an SIEM solution, Netsurion Open XDR 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 Netsurion Open XDR Monitoring Features

2.1 Reports Insertion/Removal of the Removable Devices

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

2.2 Prevents Unauthorized Access and Reports the Intrusion in Real-time

Every time a USB is inserted, the Netsurion Open XDR agent looks at the USB exception list, and if there is no violation of policy, it permits access to the device, while logging the insert activity. If a violation of policy is detected, access will be restricted, and the violation will be immediately sent to the Netsurion Open XDR Web console. At this point, if access is permitted, Netsurion Open XDR also begins to monitor all the activities of the device, and every file written to or deleted from the device will be recorded.

2.3 Restricts Access

Netsurion Open XDR can restrict access to all the USB devices on a system and can exempt the specified USB devices from monitoring which are added to the USB Exception list.

2.4 Protects the System from Malware

Netsurion Open XDR 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, Netsurion Open XDR logs the USB communication in detail as incidents.



Event Properties	? 🗙
Event	
Date: 11/11/2011 <u>S</u> ource: EventTracker Ti <u>m</u> e: 5:40:01 PM Category: Disk Typ <u>e</u> : Information Event <u>I</u> D: 3243 <u>U</u> ser: TOONS\sonal C <u>o</u> mputer: MCLOON	 ↑ ↓ □
Description: Detected new drive <f:> Volume Label: PNPL4 Volume 1266592866 Volume ID: \\?\Volume(116f4852-fa5d-11e0-ab24- 0016e6917cc7)\ Type: Removable File System: FAT Device ID: US8\VID_058F&PID_6387\%6G7JFL3 Network Volume: No Description: Change affects physical device or drive.</f:>	
Da <u>t</u> a: ● <u>Bytes</u> ○ <u>W</u> ords	~
OK Cancel	Apply

2.6 Alert Notification

In Netsurion Open XDR, users can configure alerts to receive notifications upon the activities related to removable media.

≡	Netsurion. Eventifiscker			4	•
	Alerts				
а в	Configuration	lack	front Details Event Filter	Custom	2

Example: Netsurion Open XDR: USB device disabled, Media Insert alert, etc.

۹ •	Configurat	ion						lack foor Deals Lett/liber (laton Systems Actions Next	
	Alert name				Threat level			Threshold level		
	EventPackers	USB device disabled			ferious		~	Medium		~
	Applies to				Aletvesion					
	[verthacker]	7.0 and later			10					
	Log Type	Event Type	Category	Event Id	Source	User	Match in De	escription	Description Exception	
			0	3242	EventTracker					
										Finish Cancel
	Netsurior	. EventTracker			lerver Time: Oct 28 02:20 AM		Response 0.597 secs		© 1999 - 2019 EventTracker	

2.7 Configures Media Insertion Report

Netsurion Open XDR has a provision to configure the reports to analyze the removable media device activities. These reports help identify unauthorized access to the systems. To configure the USB device report, open **Netsurion Open XDR > Operations > Reports**. In the **Report Tree**, click the **USB Device Report** node.



Reports W	/izard - Selection
Select Categ	jory/Reports to Configure
Report Type	e: 🔿 On Demand 🔿 Queued 💿 Scheduled 🔿 Defined
Security	Operations Compliance Flex reports Alphabetical Favorites
Let b	Indusion Detection System
-1	ITS ACS Metrics Report
i i i i i i i i i i i i i i i i i i i	Log on/off Activity
i i i i i i i i i i i i i i i i i i i	Netflow Report
i i i i i i i i i i i i i i i i i i i	Network Traffic
-1	Password Reset Report
÷.	Performance
In the second	Printer Usage
	RSA SecurID report
-1	Service Downtime
In the particular of the pa	Software Maintenance
÷.	StatusTracker Resource Summary
-1	System shutdown
(USB Device Disabled Report
i in t	USB Device Report
	USB Device Report Detail
	USB Device Report Summary
	Juser Activity
1	

3 Enabling Removable Media Monitoring Feature

- 1. When a USB device is plugged in or media is inserted into the CD/DVD drive, Windows sends a media insertion notification with the drive name to the Netsurion Open XDR Windows Agent.
- 2. Upon receiving the notification, Netsurion Open XDR Windows Agent launches **USBTracker.exe** with drive details. **USBTracker.exe** is a Netsurion Open XDR utility that monitors removable media file change activities.
- 3. **USBTracker.exe** generates **Event 3239** and starts monitoring all the 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 of all activities.

Note

This feature is supported by Windows only and requires Netsurion Open XDR Agent to be installed and configured.



3.1 Monitoring CDW/DVD Burning Activities

Windows has a built-in CD recorder feature that lets to 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 ".

3.2 Monitoring CD-ROM Activities

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

3.3 Configuring Netsurion Open XDR Agent to Monitor Removable Media

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

📮 EventTracker Agent File Help	Configuration		
Select Systems			
ETTVMBLR22016-4		 Agent based system 	n
Apply the following	ng settings to specified Ad	aents	
ETTVMBLR22016-4			
Log Backup	Performance	Network Connections	
Logfile Monitor Fi	le Transfer syslog F1	P server Suspicious Acti	vity
Managers Event Fil	ters System Monitor	Monitor Processes Serv	ices
CPU Performance	e (%): 90 💌 <): 90 💌		
🔽 Disk Space:	O Used more that	n (%): 80 🔽	
Advanced	 Free less than (MB): 5120	
USB and other Devi	ce Changes:		51
Report insert/ren	nove		
🔲 Disable USB D	evices 🔽	Record activity	
Mass Storage	e Devices	LISB Exception List	
C All Devices	_	2	
C All Devices (F	xcept Human Interface [Devices Class)	
	10		



Note

This option will report the device detected and device removal of Event IDs 3228 and 3229 for USB/Pen drives/External CDs, DVDs, etc. It will not report device detection and removal for mobile devices/External hard disk/Keyboard/Mouse.

3.3.1 Record Activity

Enabling this option will record the add/modify/delete activities from the hard disk to external devices. An Event ID 3240 will be generated. The supported devices are **Pen Drives, CDs, and DVDs.**

USB and other Device Changes:	
✓ <u>Report insert/remove</u>	
Disable USB Devices	Record activity
Mass Storage Devices All Devices	USB Exception List
C All Devices (Except Human Int	erface Devices Class)
Save	Close

Note

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

3.3.2 Disable USB Devices

- a. **Mass Storage Devices:** It will disable Pen Drives/External CDs or DVDs/Hard disks and Mobile devices (having Flash Drives and which do 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 the 2.0 series.
- All Devices: It will disable Pen drives/External CDs or DVDs/Mouse/USB Headphones/ USB External CDs or DVDs except Keyboard.
- c. All Devices (Except Human Interface Devices Class): All devices such as Pen drives/External CDs or DVDs/Mouse/USB Headphones/ USB External CDs or DVDs will be displayed except Human Interface Devices (HIDs) which include Keyboard, Mouse, Joystick and Numeric Keypad.

Tebercanero	
Disable USB Devices	Record activity
Mass Storage Devices	USB Exception List
C All Devices	(=
C All Devices (Except Human	Interface Devices Class)



4 Exempt Authorized USB Drives

This option helps to restrict the users to use only authorized USB devices. Click the **USB Exception List**. Netsurion Open XDR enables this button only when you select the disabled USB devices checkbox. Netsurion Open XDR displays the USB Exception List pop-up window. The USB Exception list is divided into two sections:

4.1 USB Volume Serial Number

It will work for devices that possess volume levels 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.

Netsurion Open XDR adds the newly entered volume serial number to the exception list.

🕎 USB Exception List >
USB Serial Numbers (Decimal/Hexadecimal format)
USB devices with following volume serial numbers will not be disabled when inserted.
123154545456 (0 ×1CAC953B30)
Format
Enter USB Volume Serial No :
Add <u>E</u> dit <u>B</u> emove
 Device identifiers(Device id/Hardware id/Class GUID) USB devices with following Device identifiers or Hardware identifiers or Class GUID will not be disabled when inserted.
Enter USB identifiers :
Add Edit Remove
Cancel Save & Close

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 name for the USB device.
- 3. Open the command prompt and type the <drive name> of the USB drive.
- 4. Type "dir" to see the directory listing.



C:WHOWSeysteen32emd.exe	- O ×
Microsoft Windows XF (Version 5.1.2600) (C) Capyright 1905-2001 Microsoft Carp.	-
C:\Decuments and Settings\Senal)F:	
F:\>dir Uolume in drive F is PNPL4 Uolume Serial Number is D8EF-95E8	
Directory of Fix	
File Not Found	
ris con	
	-

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

USB Exception List				
USB Serial Numbers (Decimal/Hexadecimal format)				
USB devices with following volume serial numbers will not be disabled when inserted.				
2186692866 [0 X82564902]				
C Dec				
Enter LISB Volume Serial No :				
Add Ldit Hemove				
Device identifiers(Device id/Hardware id/Class GUID)				
USB devices with following Device identifiers or Hardware identifiers or Class GUID will not be disabled when inserted.				
Enter USB identifiers :				
Add Eth Barraya				
<u>C</u> ancel <u>S</u> ave & Close				

Note

- In the Command prompt, the volume serial number will always be in the 'Hexadecimal' format. You can convert it into Decimal format if required.
- It works only for Pen drives 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 number in the USB Volume Serial No field.

- USB Serial Numbers (Decimal/Hevadecimal format)
USB devices with following volume serial numbers will not be disabled when inserted.
Format
◯ <u>D</u> ec
Enter USB Volume Serial No : D8EF95E8
Add Edit <u>R</u> emove

2. To convert the number into decimal format, click the **Dec** option. Netsurion Open XDR automatically converts the number from Hexadecimal to Decimal format.

	F	ormat • Dec	⊂ <u>H</u> ex
Enter USB Volu	me Serial No : 36	39580136	
Add	<u>E</u> dit	<u>R</u> emove	

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

Note

Netsurion Open XDR will not allow you to enter an invalid number (containing an alphabet or symbols) 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.

Device ID

It differs for all the devices. To add the Device ID to the exception list, perform the following steps:

1. Right-click **Computer** and select **Manage**.





2. Select Device Manager.

Note

Based on the device, select from the listed options.

3. When the latest Android version mobile phones are connected, they will be displayed as "Portable Devices ". The screen is shown below:



4. When the Android mobile phones of earlier versions such as 2.0 (with Flash devices) are connected, it will display within the **USB Mass Storage Device**. Here we have shown an example of a USB Mass storage Device.



E Computer Management (Local	a 🚓 Casper	Actions	_
System Tools	⇒ d∰ Computer	Device Manager	
C Task Schedder C Task Schedder C Task Schedder Sched Folder Sched Folder Defermance Dock Management Services and Applications	Disk drives Disk drives Disk drives Disk drives DVD/CD-ROM drise DVD/CD-ROM drives DVD/CD-ROM drives	Mere Actiona	

- 5. Right-click the USB Mass Storage device. Select Properties.
 - Universal Serial Bus controllers
 Generic USB Hub
 Generic USB Hub
 Standard Enhanced PCI to USB Host Controller
 Standard Enhanced PCI to USB Host Controller
 USB Most H Update Driver Software...
 USB Root H Update Driver Software...
 USB Root H Enable
 Uninstall
 Scan for hardware changes
 Properties
- 6. The USB Mass Storage Device Properties page will be displayed as shown below:
 - a. Select the **Detail** tab.
 - b. In the Property option, select Device Instance Path from the dropdown list.

USB Mass Storage Device Properties
General Driver Details
USB Mass Storage Device
Property Device Instance Path
Value USB\VID_03F0&PID_5A07\AEA09H02YE11000108
OK Cancel



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

Device identifiers(Device id/Hardware id/Class GUID) USB devices with following Device identifiers or Hardware identifiers or Class GUID will not be disabled when inserted.
Enter USB identifiers :
Add Edit Remove
Cancel Save & Close

7. Click the **Add** button.

🔛 USB Exception	n List 💽
USB Serial Numbers (Decimal/Hexadecimal format)	
USB devices wi	th following volume serial numbers will not be disabled when inserted.
	Format
	● <u>D</u> ec ○ <u>H</u> ex
Enter USB Volu	ne Serial No :
Add	<u>E</u> dit <u>R</u> emove
Device identifiers USB devices wi not be disabled	(Device id/Hardware id/Class GUID) th following Device identifiers or Hardware identifiers or Class GUID will when inserted.
USB\VID_03F0	0%PID 5A07\AEA09H02YE11000108
Enter USB ident	ifiers :
Add	<u>E</u> dit <u>R</u> emove
	<u>Cancel</u> Save & Close

Possible Substring Match for Device ID

The **disabled USB Devices** checkbox when clicked blocks the entry of all the USB devices. However, for authentic USB devices, we can add their USB serial number or Device ID to allow the USB data transfer. The following are the possible substring matches 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 the 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 <u>here</u> for more details on PID/VID.

Hardware ID

Hardware ID remains the same for a device of the same class type but different for other class types. (e.g., the Hardware ID of the optical mouse will be the same, but the hardware ID of Lenovo, Dell, or HP will differ from each other). To add the Hardware ID to the exception list, perform the following steps:

1. Select the Hardware ID from the dropdown list in the Property section.

USB Mass Storage Device Properties
General Driver Details
USB Mass Storage Device
Property
Hardware Ids
Value
USB\VID_03F0&PID_5A07&REV_1100
OK Cancel

- 2. Copy the value and paste it in the **Device identifiers** field.
- 3. Click the **Add** button. It gets added and will be displayed as shown below:

🖼 USB Exception List
USB Serial Numbers (Decimal/Hexadecimal format)
USB devices with following volume serial numbers will not be disabled when inserted.
Format © Dec O Hex
Add Edit Remove
Device identifice(Device id/Hardware id/Class GUID)
USB devices with following Device identifiers or Hardware identifiers or Class GUID will
not be disabled when inserted.
USB\VID_03F0&PID_5A07&REV_1100
Enter USB identifiers :
Add Edit <u>R</u> emove
Cancel Save & Close



Class GUID

Class GUID remains the same for a device class. (e.g. class GUID of the optical mouse will be the same for all whether it is Lenovo, Dell, or HP). The following is a table with the devices and their respective values.

Device	Value
Battery	{72631e54-78a4-11d0-bcf7-00aa00b7b32a}
Biometric device	{53D29EF7-377C-4D14-864B-EB3A85769359}
Bluetooth	{e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
CDROM	{4d36e965-e325-11ce-bfc1-08002be10318}
Disk Drive	{4d36e967-e325-11ce-bfc1-08002be10318}
Display Device	{4d36e968-e325-11ce-bfc1-08002be10318}
FDC	{4d36e969-e325-11ce-bfc1-08002be10318}
Floppy Disk	{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}

Device	Value
Infrared	{6bdd1fc5-810f-11d0-bec7-08002be2092f}
Keyboard	{4d36e96b-e325-11ce-bfc1-08002be10318}
Medium Changer	{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 disabling the mobile devices.

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

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

To add Class GUID to the exception list, perform the following steps.

1. Select **Device Class GUID** from the dropdown list.



USB Mass Storage Device Properties
General Driver Details
USB Mass Storage Device
Property
Device class guid
Value
{36fc9e60-c465-11cf-8056-444553540000}
OK Cancel

- 2. Copy and paste the value in the **Device Identifier** field.
- 3. Click the Add button.

SB Exception List
USB Serial Numbers (Decimal/Hexadecimal format)
USB devices with following volume serial numbers will not be disabled when inserted.
Format
(<u>● D</u> ec (<u>∩ H</u> ex
Enter USB Volume Serial No :
Add Edit Berrove
Device identifiers(Device id/Hardware id/Class GUID)
USB devices with following Device identifiers or Hardware identifiers or Class GUID will
not be disabled when inserted.
{36fc9e60-c465-11cf-8056-444553540000}
Enter LISP identifiere :
<u>Add</u> <u>E</u> dit <u>R</u> emove
Cancel Save & Close

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

4.4 Configure Device Monitoring Alerts

The Device Monitoring Alerts can be configured to receive notifications. You can also view these Alert events on the Alerts Dashboard.

4.4.1 Configure USB Device Monitor Alerts

- 1. Click Admin and then select Alerts.
- 2. Locate Netsurion Open XDR: USB device disabled & Media Insert Alerts.
- 3. Select the severity of the threat from the Threat Level dropdown list.
- 4. Select the checkbox under Active, if not selected.
- 5. Set appropriate alert actions to receive notifications.
- 6. Click **OK**.



≡	Netsurion.	EventTracker'							ø	Admin •	Tools +	🔘 Maheshwar Reddy
•	Alerts											🕈 / Admin / Alerts / Wizar
۹	Configurati	ion						Back Event Details Event Filte	r Custom Sy	stems Action	s Next	
k	- T											
	Alert name				Threat level			Threshold level				
	EventTracker: I	USB device disabled			Serious		~	Medium				~
	Applies to				Alert version							
	EventTracker 7	1.0 and later			1.0							
	Log Type	Event Type	Category	Event Id	Source	User	Match in D	Description	Descriptio	n Exception		
			0	3242	EventTracker							
												Finish Cancel

≡	Netsurion EventTracker						
	Alerts						
Q B	Configuration						Back Event
	Alert name			Threat level			Threshold level
	Media insert alert			High		~	Medium
	Applies to			Alert version			
	EventTracker 7.0 and later			1.0			
	Log Type Event Type	Category	Event Id	Source	User	Match in De	scription
		0	3228	EventTracker			

4.5 Netsurion Open XDR Device Monitoring Categories

To view Categories, click Admin and then select Category.

Category: Netsurion Open XDR: USB device disabled **Description:** All the events logged by Netsurion Open XDR when it disables the unauthorized USB devices, which is not in the exception list. **Event ID:** 3242



≡	Netsurion EventTracker							
	Category							
Q R	Category Tree Search	Category De Parent Group EventTracker Description All events log	tails gged by EventTracke	er when it disables	: unauthorized U	ISB device, which is n	ot in the exc	ception list. Event ld: 3242
	EventTracker: System group created EventTracker: System group deleted EventTracker: System group modified EventTracker: System type changed EventTracker: Truncated description EventTracker: Unknown MDS hash detected	Applies to EventTracker 7.0 and later Show In Operations Compliance Security Event Rule						
	EventTracker: Usage data submission failed	Log Type	Event Type	Category	Event Id	Source	User	Match in Description
	EventTracker: USB of exter disabled EventTracker: USB of the device disabled EventTracker: USB or other device monitoring EventTracker: VCP port added EventTracker: VCP port modified EventTracker: VCP port modified EventTracker: Vulgentage added EventTracker: Weightage deleted EventTracker: Weightage deleted EventTracker: Weightage deleted EventTracker: Weightage deleted EventTracker: Weightage modified EventTracker: Weightage modified EventTracker: Weightage: Model with add clear	0	0	0	3242	EventTracker		

Category: Netsurion Open XDR: USB or other device monitoring

Description: All events logged by Netsurion Open XDR while monitoring USB, CD, and DVD devices or media insertion and removal.

Event ID: 3228, 3229, 3239, 3240.

≡	Nétsurion EventTracker									*	Admin -	Tools •	🔘 Mah	eshwar Red
	Category												† / A	imin / Cate
 Q. B.	Category The Search Comparison of the subport of research corrections Comparison of the subport of research corrections Comparison of the subport of research Comparison of the research Comparison of	Category Det Parent Group EventTracker Description All events log EventTracker Show In 🕑 Event Rule Log Type 0 0 0	ails ged by EventTracke 7.0 and later Coperations Cope	r while monitoring compliance 5 Category 0 0 0	g USB, CD, and E iecurity Event Id 3228 3229 3240	VD device or media	insertion ar	nd removal. Event Id: 3225 Match in Description	Deent Category Name TeverEnctere USE or ather device monitoring A 3228, 3248, 3228 Category version 10 Description Exception	Lucene Query (event, dd.3228 AND eve (event, dd.3228 AND eve (event, dd.3228 AND eve	nt_source"Eve nt_source"Eve	Ar intTracker*) intTracker*)	dd 🗍 Edit	Delete
I	Eventrace: V> por asses Eventrace: V> por neates Eventrace: V> por neates Eventrace: V> por neates Eventrace: V> porting	0	0	0	3239	EventTracker				(event_id:3239 AND eve	ent_source:"Eve	entTracker")	Save	Cancel

4.6 Netsurion Open XDR Device Monitoring Reports

4.6.1 USB or Other Device Monitoring

Go to Operations > Reports > Netsurion Open XDR: USB or other device monitoring.

Netsurion Open XDR 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 selected period.



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



Category Detai	l Report Sorted	By Compu	ıter	
Category EventTracker	: USB or other device mo	onitoring had 1	Computers gener	ating 22 events
Event IDs included are 32	228, 3229, 3239, 3240			
Computer FELIX generate	d 22 events. Details of Ever	nts are given belo	w.	
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 1D: \\?\Volume(8c5f0eaa-f5d0-11e4 -bf06-fcf286e6e67f)\ File System: NTF5 Device ID: USB\VID_0BC2&PID_5021\NA05SA8] Network Volume: No Description: Change affects physical device or drive. <eventdata><detected ⁢f:><br="" drive="" new="">Device Type: Fixed Volume Label: FreeAgent GoFlex Drive Volume Serial No: 1546817573 Volume ID: \\?Volume(8c5f0eaa-f5d0-11e4 -bf06-fcf286e6e67f)\</detected></eventdata></f:>
9/7/2015 3:14:45 PM	J	3229	EventTracker	File System: NTFS Device ID: USB\VID_OBC28amp;PID_5021\NA05SA8J Network Volume: No Description: Change affects physical device or drive. Drive. <f:> removed.</f:>
				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>



4.6.2 USB Device Disabled Report

Go to **Operations > Reports > USB Device Disabled Report.**

This report provides information on the disabled USB devices across selected computers for the selected 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		USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:42:48PM	/	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:43:25PM	/	USB Mass Storage Device	USB\VID_0951&PID_1629\0018F30C9F
9/9/2015 6:44:13PM	AND 171	USB Mass Storage Device	USB\VID_0BC2&PID_5021\NA05SA8J
9/9/2015 6:44:42PM		USB Mass Storage Device	USB\VID_0BC2&PID_5021\NA05SA8J
9/9/2015 6:49:10PM	ANNETT	USB Input Device	USB\VID_17EF&PID_6019\6&25e9f07&(
9/9/2015 6:54:07PM	ANDITI	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&
9/9/2015 6:54:12PM	AMPITI	USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:55:07PM		USB Input Device	USB\VID_0461&PID_4E22\6&25e9f07&(
9/9/2015 6:59:30PM		MTP USB Device	USB\VID_0FCE&PID_0180\YT9100L4LK

4.6.3 USB Device Report Details

Go to 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.

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

uter FELIX Removable media devices used is 1						
\DVD Device (E:\) with Seria	al No. 2663209342 a	active users is 1				
Active Users: TOONS	file activities is 8					
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				

4.6.4 USB Device Report Summary

Go to **Operations > Reports > USB Device Report > USB Device Report Summary.**

This report provides a summary of the files added/modified/deleted to the USB device. The charts are included per system per activity, top 10 USB devices are 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.





4.7 Netsurion Open XDR Generated Events

Netsurion Open XDR detects the new drive [3228]



Details: 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 drives.



Netsurion Open XDR <drive name> removed [3229]

Drive <f:> remo Netwo Descrip</f:>	wed. rk Volume: No stion: Change affects phys	ical device or drive.		
I Log Name:	Application			
Source:	EventTracker	Logged:	9/7/2015 3:14:45 PM	
Event ID:	3229	Task Category:	(2)	
Level:	Information	Keywords:	Classic	
User:	TOONS\akriti	Computer:	Felix.Toons.local	
OpCode:				
More Informatio	n: Event Log Online Help	2		

Details: Drive <F:> removed Network Volume: No Description: Change affects physical devices or drives.

USB device is disabled by Netsurion Open XDR [3242]

USB Device is o Devic Devic Devic Devic Devic Drive Devic	disabled by EventTracker. F e Type: USB Device e ID: USB\VID_0BC2&PID_ e Description: USB Mass St e Friendly Name: N/A r: {36fc9e60-c465-11cf-805 e ClassGUID: {36fc9e60-c44	Please contact your syst 5021\NA05SA8J corage Device 6-444553540000}\0007 55-11cf-8056-444553540	em administrator. 0000}	•	
Log Name:	Application				
Source:	EventTracker	Logged:	9/7/2015 3:16:17 PM		
Event ID:	3242	Task Category:	(2)		
Level:	Information	Keywords:	Classic		
User:	TOONS\akriti	Computer:	Felix.Toons.local		
OpCode:					
More Informati	on: Event Log Online Hel	lp.			

Details: USB Device is disabled by Netsurion Open XDR. 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]

Deficial Detail	5				ĩ
Drive Monitor	ing started for E:\			<u> </u>	
Devi	e Type: CD/DVD				
Volu	me Label: Aug 24 2015 me Serial No: 2663209342			=	
Volu	me ID: \\?08f823c	13-f5d0-11e4-bcaa-806e6	of6e6963}\		
File S	ystem: UDF				
Devi	te ID: N/A			Ŧ	4
Log Name:	Application				
Source:	EventTracker	Logged:	9/7/2015 3:47:42 PM		4
Event ID:	3239	Task Category:	(2)		
Level:	Information	Keywords:	Classic		
User:	N/A	Computer:	Felix.Toons.local		
OpCode:					
More Informat	on: Event Log Online He	dp			

Details: 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 the drive. Console User: TOONS\akriti Active Users: TOONS\akriti



USB Monitoring stopped for<drive name> [3240]

Drive Monitor	ing stopped for E:\			*	
Devie	ce Type: CD/DVD				
Volu	me Label: Aug 24 2015				
Volu	me ID: \\?08f823d	B-f5d0-11e4-bcaa-806e6	if6e6963}\		
File S	ystem: UDF				
Devi	ce ID: N/A			-	
Log Name:	Application				
Source:	EventTracker	Logged:	9/7/2015 3:45:40 PM		4
Event ID:	3240	Task Category:	(2)		
Level:	Information	Keywords:	Classic		
User:	N/A	Computer:	Felix.Toons.local		
OpCode:					
	5 11 5 11	1.11			

Details: 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 the 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\akritidesktop.ini | Existing | 09/07/2015 02:23:19 PM

4.8 Limitations

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



About Netsurion

Netsurion[®] delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at <u>www.netsurion.com</u>.

Contact Us

Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers SOC	C@Netsurion.com
Managed XDR Enterprise MSPs SOC	C-MSP@Netsurion.com
Managed XDR Essentials Esse	entials@Netsurion.com
Software-Only Customers Soft	ware-Support@Netsurion.com

https://www.netsurion.com/support