

IT USB Drive

Detected usage of same unauthorized USB drive in Mr. Buongiorno workstation and Training Center computer

VID_0781 PID_5581

The screenshot shows the Windows Device Manager interface. The left pane displays a tree view of hardware categories, with 'USB' expanded to show various USB hubs and storage devices. The right pane shows the properties for a selected USB drive, displaying a list of registry values.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000001 (1)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{eee5ad10-332d-59e1-8733-d85521a30cb8}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
FriendlyName	REG_SZ	SanDisk Ultra USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskSanDisk_Ultra_____1.00 USBSTOR\DiskSanDisk
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

- WAN Miniport (Network Monitor)
- WAN Miniport (PPPOE)
- WAN Miniport (PPTP)
- WAN Miniport (SSTP)
- Other devices
 - Base System Device
- Portable Devices
- Ports (COM & LPT)
- Print queues
- Processors
- Software devices
- Sound, video and game controllers
- Storage controllers
- System devices
- Universal Serial Bus controllers
 - Generic USB Hub
 - Generic USB Hub
 - Standard Enhanced PCI to USB Host Controller
 - Standard Universal PCI to USB Host Controller
 - Standard USB 3.0 eXtensible Host Controller
 - USB Composite Device
 - USB Mass Storage Device
 - USB Root Hub
 - USB Root Hub
 - USB Root Hub (USB 3.0)

USB Mass Storage Device Properties

General Driver **Details** Events Power Management

USB Mass Storage Device

Property: Device instance path

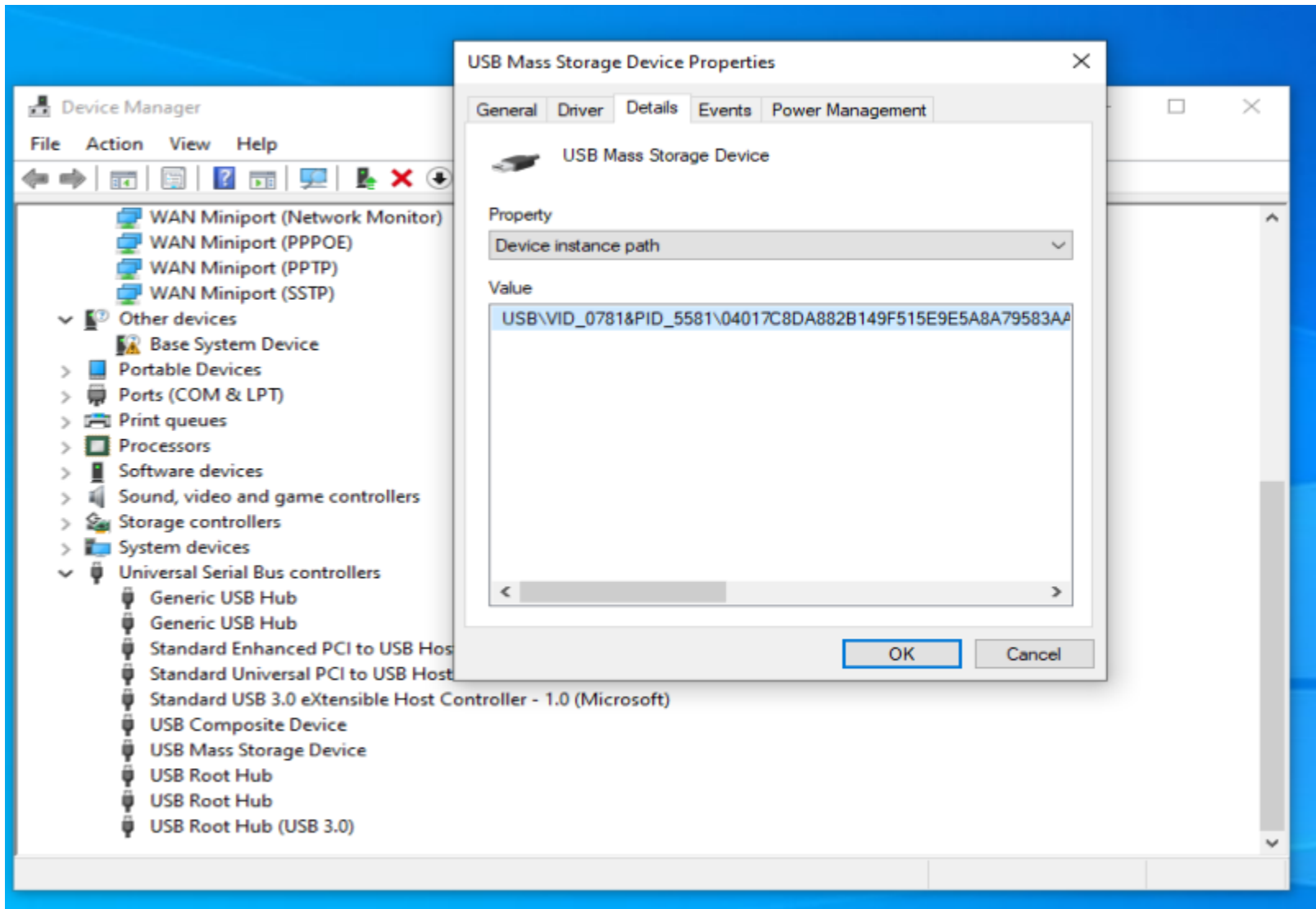
Value: USB\VID_0781&PID_5581\04019E54B0EF226876F7073C5CFB84C7081

OK Cancel

RM USB Drive VID_0781 PID_5581

The image shows the Windows Registry Editor. The left pane displays the tree structure, with the path `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00\04017c8da882b149f515e9e5a8a79583aa9ab8fdb1235777e9bf8c661aac660` selected. The right pane shows the registry values for this key:

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000001 (1)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11c1
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBS
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{6bcc7c26-21d1-5cb
DeviceDesc	REG_SZ	@disk.inf,%disk_dev
Driver	REG_SZ	{4d36e967-e325-11c1
FriendlyName	REG_SZ	SanDisk Ultra USB Dr
HardwareID	REG_MULTI_SZ	USBSTOR\DiskSanDi
Mfg	REG_SZ	@disk.inf,%genman
Service	REG_SZ	disk



CS USB Drive VID_0781 PID_5581

Registry Editor

File View Favorites Help

ter\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00\0401e4c73a474241ccc01df05d1ab6e512a0e1c0477f336b303d450e3742e62

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000001 (1)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{0736e9f7-9064-59f5-93e6-b35f656724a3}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
FriendlyName	REG_SZ	SanDisk Ultra USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskSanDisk_Ultra_____1.00
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard
Service	REG_SZ	disk

