Virenschutz

Symantec Endpoint Protection: USB-Sperre einrichten

A) **Gather the Device ID of device(s) to exclude using the DevViewer tool:**
1. Find the DevViewer.exe tool on the SEP 11.0.X CD2 in the CD2\Tools\DevViewer folder.
2. Plug in the device you want to gather the Device ID from.
3. Run the DevViewer.exe tool and browse to find the device. (Example, for a thumb drive, look under Disk drives)
4. Select the device, and on the right you will see information about the device.
5. Right click the [device id] and select Copy Device ID.
6. Exit the DevViewer Tool.

Note: Alternative way to find Device ID in case DevViewer is not available:

1. On the Windows taskbar, click **Start > Settings > Control Panel > System**.
2. On the **Hardware** tab, click **Device Manager**.
3. In the **Device Manager** list, double-click the device.
4. In the device's **Properties** dialog box, on the **Details** tab, select the Device ID (on Windows XP) or Device Instance Path (Windows Vista or 7).
5. Press **Control+C** to copy the ID string.

In case of difficulties in finding the correct 'Device ID' for building the rule, please remember that in DevViewer you may change 'View Style' to "View devices by connection", which may help, particularly when troubleshooting USB exclusions.

B) **Add the Hardware Device into SEPM policy:**
1. In the SEPM, select the Policies view.
2. In the upper left corner of the console, under the View Policies section, click on Policy Components to expand the sub-list.
3. Under Policy Components, select Hardware Devices.
4. Under Tasks, select Add a Hardware Device
5. Type in the Name you wish to call your device (example: Administrator's Thumb drive).
6. Select the Device ID option, click in the text box and use CTRL-V to paste the Device ID you copied from the DevViewer tool.
7. Click **OK**.

C) **Add Disk Drives and the Hardware Device to allow to the Devices Excluded From Blocking list:**
1. In the SEPM, Under View Policies, select Application and Device Control
2. Right click your Application and Device Control Policy and select **Edit**.
3. There are 2 ways to correctly implement a block and exclusion.
a. Either accomplish the blocking and exclusion via Device Control or Application Control.
b. **Do not use a mix of the 2 methods to block and exclude devices.**

D) **To use Device Control:**
1. Select the Device Control view.
2. Under the Blocked Devices section, click **Add**, select Disk Drives and click **OK**. (If Disk Drives isn't listed, it is already added as a Blocked Device).
3. Under Devices Excluded From Blocking, click **Add**.
4. Select the device you added in the previous section and click **OK**.
5. Click **OK** to the Application and Device Control policy window.

E) **To use Application Control:**
1. Select the Application Control view.
2. Select (Check Mark) "Make all removable devices read-only" (For example) and select **Edit**.
3. Select "Block writing to all files and folders", under "Do not apply to the following files and folders", select **Add...**
4. Under "File or Folder Name To Match" enter a * (An Asterisk).
5. Select (Check mark) "Only match on the following device id type", press **Select.**
6. Select (Highlight) the device added to the hardware list (The unique USB device added previously.) and press **OK.**
7. Press **OK** to close windows until at the "Application and Device Control Policies" window of the SEPM.

Select "Assign the Policy"
Select the group to assign the edited policy to.
Press "Assign"

Standard Class-IDs:

- Disk Drives - {4d36e967-e325-11ce-bfc1-08002be10318}
- Storage Volumes - {71a27cdd-812a-11d0-bec7-08002be2092f}
- USB devices - {36FC9E60-C465-11CF-8056-444553540000}
- DVD/CD-ROM - {4D36E965-E325-11CE-BFC1-08002BE10318}
- IDE - {4d36e96a-e325-11ce-bfc1-08002be10318}
- PCMCIA - {4d36e977-e325-11ce-bfc1-08002be10318}

Sinnvolle Praxisbeispiele mit wildcards:

Any USB Storage device

- USBSTOR*

Any USB Disk

- USBSTOR\DISK*

Any USB SanDisk drive

- USBSTOR\DISK&VEN_SANDISK*

Any USB SanDisk Micro Cruzer drive

- USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO*

A specific SanDisk device

- USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0

Link: https://support.symantec.com/en_US/article.TECH175220.html

Eindeutige ID: #1185
Verfasser: Uwe Kernchen
Letzte Änderung: 2016-03-17 09:56