Control USB devices using Group Policy

This article will show you how to use Device Installation Restrictions to control USB devices in Windows Vista.

Network Administration - *When it comes to security, network protection, corporate data protection, or similar issues on your corporate network, there's one thing you have to think about that is how to control it. USB and hard drives. If the user can bring the USB to the office (can be easily pocketed), copy all the secret files in, then plug the USB into another of their desktop for copying or real Executing files from a USB, the exposure for an attack or virus infection may occur at any time. Until now, the control of USB devices is still very limited. However, Microsoft introduced a new feature called Device Installation Restrictions to control USB devices in Windows Vista. These settings are quite easy to configure, control and very powerful when they are deployed with Group Policy.*

Consider two scenarios that control USB devices

Restricting USB devices takes place in two scenarios. The first scenario is quite simple because it relates to computers that have never known USB devices before. In such a case, the computer does not have any USB devices installed. The second scenario is when the USB device is installed. In this case, the USB has been configured in the registry and its driver has been copied to the computer.

Control the installation of USB devices on operating system versions before Windows Vista

When there is no Windows Vista operating system, or want to verify the process of controlling the installation of USB devices on Windows 2000 or Windows XP, we want to add the capabilities that you have for these operating systems. This process allows you to control USB devices but is not easy to deploy or control compared to the new option of controlling USB devices using Group Policy.

With Windows 2000 and XP, you need to change the existing file permissions to limit the installation of USB devices. The two files you need to change here are USBSTOR.PNF and USBSTOR.INF, both of which are in the *% systemroot% inf directory*. To refuse to install USB devices, you need to change the security on each of these files. To change the security conditions on each file, right-click the file, then select Properties. In the Properties window, select the Security tab. Then select the group name that the user is in (the name of the group you want to deny the installation of the USB device), then select the Full Control clause as shown in Figure 1.

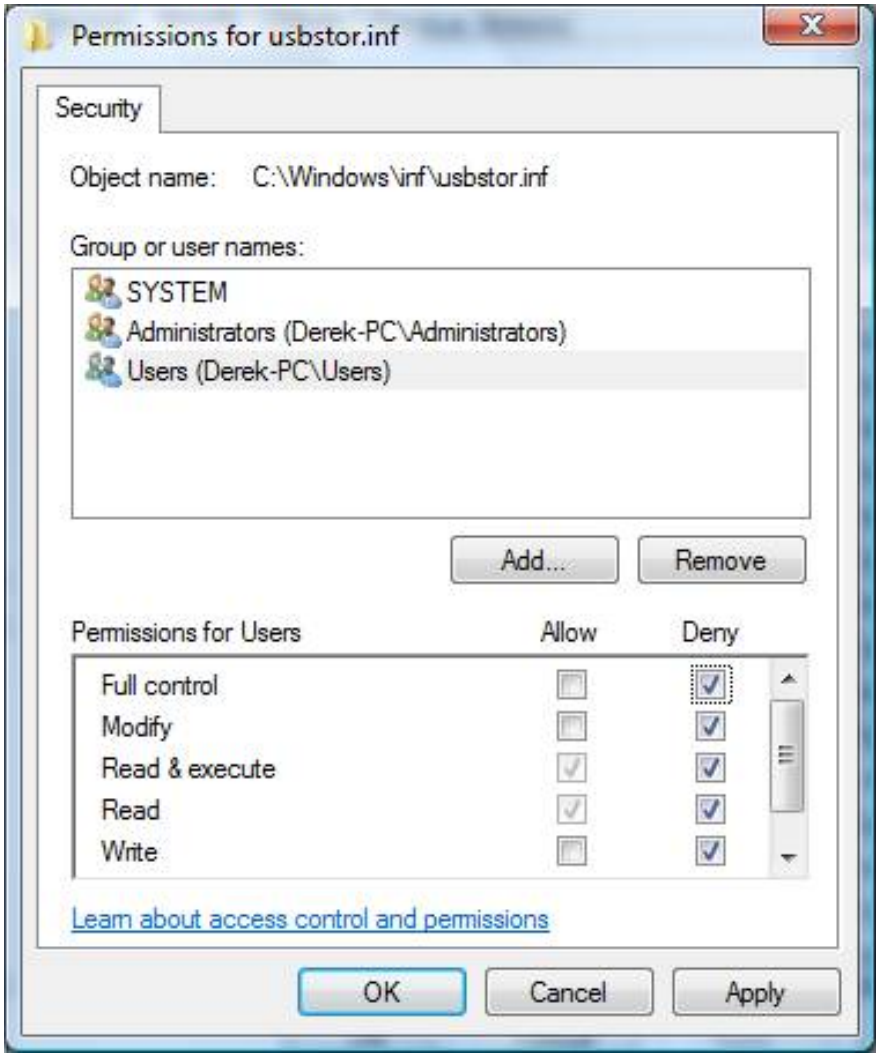

Figure 1: Configuring the group name with the terms Deny is Full Control for both files

Control USB installation on Windows Vista

With Windows Vista computers, you can use Group Policy object settings to restrict the installation of USB devices. This method provides a more refined way of controlling individual USB devices. This method is not an 'all or nothing' solution compared to methods with previous operating systems that have quite a few tweaking options. With this method, you will consider the USB ID. This ID will be used in device control policy. One advantage of a policy through Group Policy is that you can restrict the USB device or allow it. You can also set up tweaking your own conditions for what is allowed and what is not allowed. The USB ID detection is to install it. This is what you have for a test computer where you can install the device.

Below are the steps needed to find the USB device ID for the installed device.

1. Open Device Manager from Control Panel.

2. Find the device in the device list. The USB device will be located under the Disk drives section.

3. Right-click the USB device and select Properties, which opens the device's properties sheet, as shown in Figure 2.

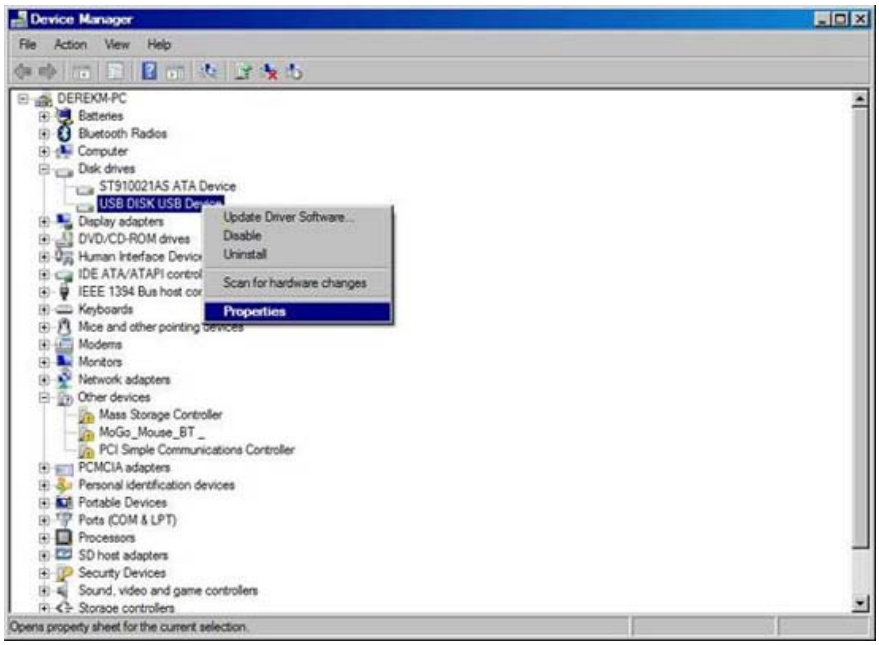

Figure 2: Select the Properties of the USB device from Device Manager

4. Select the Details tab from the USB properties sheet

5. Click on the dropdown list with the Property label

6. Select the Hardware Ids option, as shown in Figure 3.

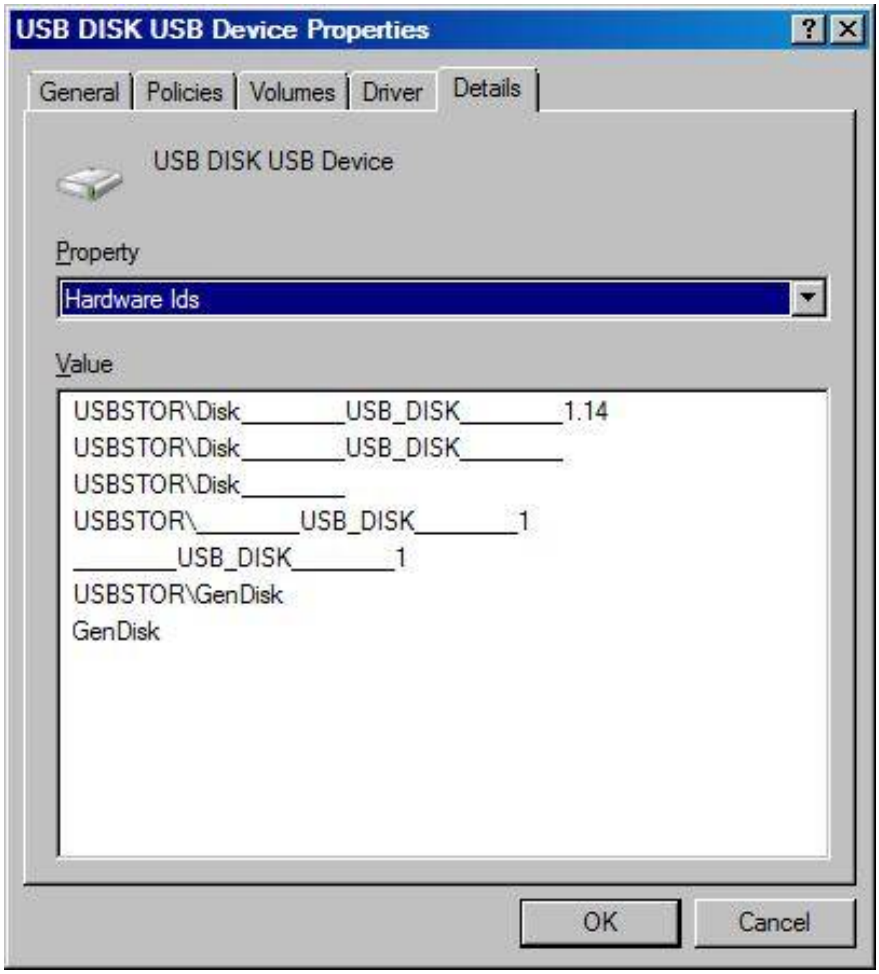

Figure 3: Device class GUID is what you will use for hardware ID

With this USB ID, you can create and configure a GPO. To configure a GPO with a USB ID and restrict device settings, follow the steps below on a computer where a USB device has not been installed.

1. Click the Start button, select Run, then type gpedit.msc, then click the OK button. (If UAC is enabled, you will have to agree to allow the Group Policy editor to run).

2. Open **Computer Configuration | Administrative Templates | System | Device Installation | Device Installation Restrictions** , shown in Figure 4.

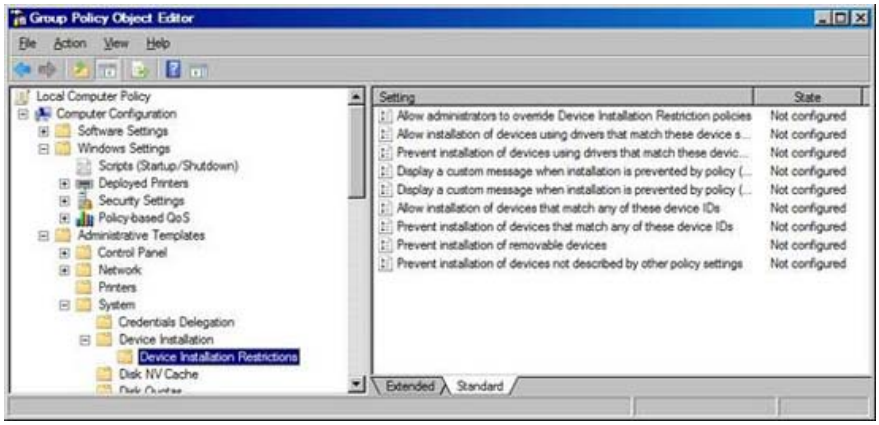

Figure 4: You will configure the policies under the Device Installation Restrictions button to control USB devices

3. Double-click the block to install devices that match this hardware ID policy.

4. Select the Enabled button.

5. Click the Show button to open the Show Contents dialog box.

6. Click the Add button in the Show Contents dialog box.

7. Type in the ID for the USB device using the syntax shown in Figure 5.

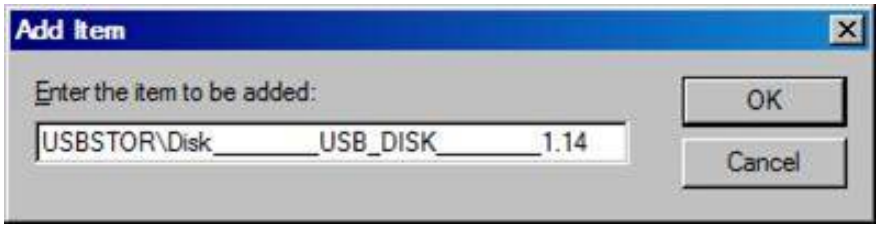

Figure 5: Policy input restricts hardware using the Hardware ID of the device

8. Save all settings within the policy and exit the editor.

At this point, you have set up your policy and can check the USB device installation. After plugging in the USB device on the computer where you configured the GPO, you will receive an error message like the one shown in Figure 6. Just click the icon in the tray to see this dialog box.

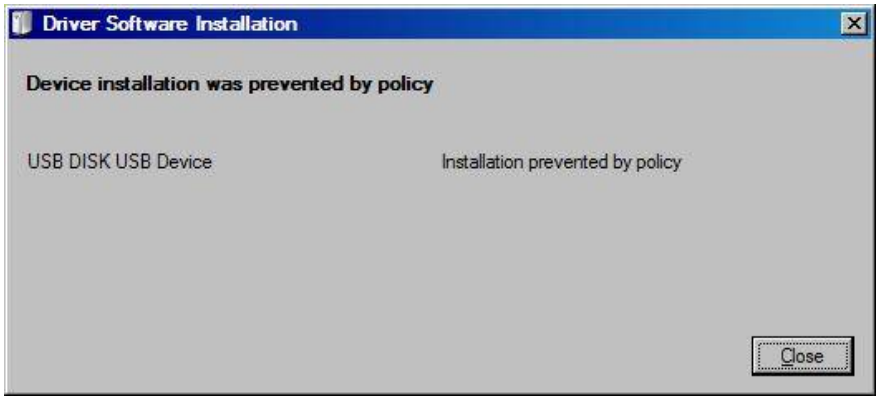

Figure 6: If the policy restricts device settings, a message will be displayed

If you want to add some information, you can also configure customizations for display notifications. There are two policies (Displaying custom messages when the installation is blocked by policy) for blocking USB IDs, you can see in Figure 4.

Note :

If the device is already installed, the policy will not refuse to run it. You will need to uninstall the device driver so this policy works, or you can use the option listed above for Windows Vista computers for the posted drivers.

Control of installed USB devices

For the second scenario, you need to consider controlling the installed USB devices. With this scenario, you have two options. The first option is to uninstall the USB drive, which will bring your computer into the state where the USB driver is not installed - because this is quite difficult to manage and cannot be executed in a large company. So choose another solution.

The second option will force you to contact the registry. Intervention in the registry can cause a blue screen error! The registry hack can be done manually, by script or even using Group Policy to deploy the setup. In this case, we recommend using Group Policy. You can also use the Registry Preference or you can customize the ADM template. Configuring the Registry Preference policy from the information in the ADM template will be quite simple! To create a template, simply copy the script below into Notepad, then save it as an ADM extension, noting that you cannot add the .txt extension to this file. Next, import this template into the GPO using the Group Policy Management Editor.

CLASS MACHINE
"Braincore.net USB Storage Drive Restriction"
POLICY "How do you want USB Drives to Behave?"
#if version> = 3
EXPLAIN "Policy to disable USB removable storage"
#endif
KEYNAME
SYSTEMCurrentControlSetServicesUSBSTOR
VALUENAME Start
VALUEON NUMERIC 3
VALUEOFF NUMERIC 4

END POLICY
END CATEGORY

Conclude

In this article we learned that USB devices can be controlled in Windows 2000, XP and Vista computers. It is possible to control the installation of these devices if they have not been previously installed, or can restrict their use if they are already installed. With Windows 2000 and XP, you have another way to limit the installation of USB devices compared to Windows Vista. Windows Vista uses GPOs, in which Windows 2000 / XP requires you to change the permissions on its files. If the device is already installed, then you will need to change the registry to limit its use. This method can be done manually or through a script or by using Group Policy. Now you can control your USB drives and your network will also be safer.