Guide to controlling device security built-in in Windows (Part 1)

In this two-part article we will show you how to protect Windows XP, Windows Server 2003 or Windows Vista from unwanted or pre-installed devices such as USB flash drives. , iPod, CD-ROM, DVD, wireless interface & he

In this two-part article we will show you how to protect Windows XP, Windows Server 2003 or Windows Vista from unwanted or pre-installed devices such as USB flash drives. , iPod, CD-ROM, DVD, wireless interface . using the features available in Windows. Let's go through the options available in Windows versions and see what they have in common and what's limited from a security standpoint.

An extended drive (or any other type) can be a blessing, but it can also be a nightmare to administer to a certain extent. With the ability to obtain a large amount of data stored on a small removable disk, it makes it an ideal tool for both users and administrators in their daily work. . However, it also causes some difficulties for the company's security policies, some people try to protect their intellectual resources or isolate them from malicious code software. The difficulty here is also caused by wireless communication, the wireless system can give you a large number of features as its 'mobility' but its weaknesses are parts. Dangerous soft code or unauthorized users can easily penetrate into your infrastructure.

With Windows XP and Windows Server 2003, in these two versions you won't get many options for pre-installed device control. However, there are still some features that can be implemented. The options available are:

Registry settings

When Windows XP SP2 was released, it had an option to make USB storage drives work only as read-only devices. By entering the Windows Registry database and **navigating** to **HKLMSystemCurrentControlSetControl** , you create a new key named **StorageDevicePolicies** . Inside this key, you create the **REG_DWORD** value named **WriteProtect** and give it a value of **1** . Done restarting the computer.

This feature does not really solve the problem raised in the article. It is only a viable solution, if you want to protect the company's intellectual resources and make it difficult for people with modest technical knowledge to copy data to a USB device. extend. However, your infrastructure still has a vulnerability in the form of being infected by malicious software stored on the primary key or maybe someone installed unauthorized software. Besides, it also only works with Microsoft own USB drives.

Group policies (Group Policies)

With external features, you only have a limited number of GPO settings that can allow you to control devices like Figure 1.

Figure 1

However, by adjusting these GPO settings you can change them to be beneficial. You can create an administrative template to disable extended storage devices introduced in the article **Disabling USB drives, CD-ROM, Floppy Disk and LS-120 using Group Policy** .

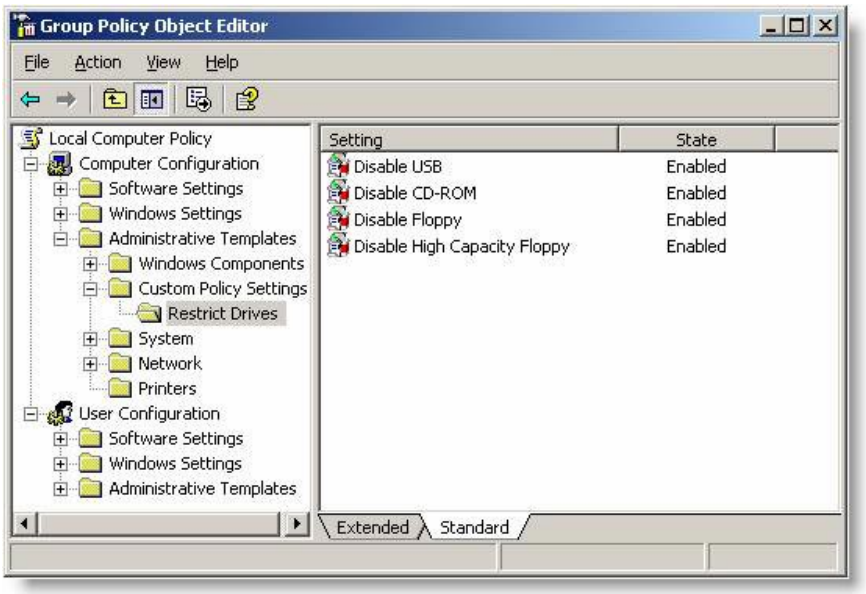

Figure 2

The secret behind this pattern is that different storage drives are disabled during the boot process. If you like, you can extend the administrator template to control other devices such as pre-installed Bluetooth drives in Windows XP SP2 and later versions.

This GPO method also has some limitations. The first is a computer-based GPO. Secondly, it is quite easy to configure as long as it is based on drives. However, it is easy to damage the administrator if you want to control specific home appliance's performance. There is a solution to this problem by making the user execute as non-administrator, the specific problem we will discuss later in this article. The third limitation is that this method can be tricked by a user to execute as an administrator. The **gpdisable.exe** tool from sysinternals.com (now part of Microsoft) can be used to disable this exception GPO with other GPOs, even if Software Restriction Policies are used. You can read more about this tool at: http://www.sysinternals.com/blog/2005/12/circumventing-group-policyas-limited.html

Allow users

If you are building a new base client from scratch, you need to have the option to control access to different storage disks based on a number of user groups. **How to disable USB drives** also introduces this issue in detail, but with the idea of ??changing permissions and denying access to one or more security groups to NPE and INF files is linked to the drive you want to control.

However, there is another way to control this is to make the user execute as if there were no administrative rights.

When a user tries to install a new hardware for the first time, he will be denied unless there are rights as shown in Figure 3.

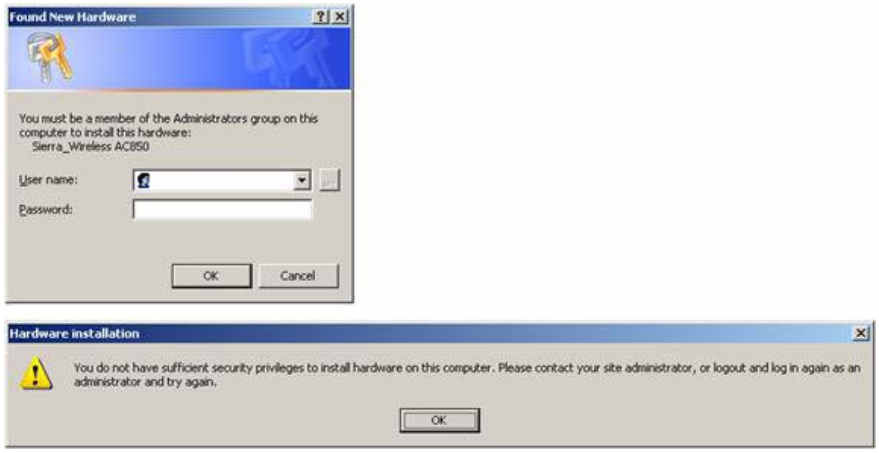

Figure 3

Disable PnP service (PnP Service)

Some administrators will perform measurements to make a decision to disable PnP Service. Normally, the PnP Service is automatically launched in Windows XP, Windows Server 2003 and also controls this service from a GPO. The advantage of this method is that it will make the computer start faster and solve the problem of device control, here it is assumed that the device is not added to the computer before this setting is possible. activated. However, it requires your deployment method to rely on a very tight deployment strategy, so this process makes it difficult to administer. The second weakness is that techniques such as evaluating two coefficients in the form of smart cards or USB cards will not work, these techniques and their tools depend on the PnP Service that started earlier.

Conclude

As you can see, there are some challenges in device control in Windows XP and Windows Server 2003, and there is no truly perfect solution for device control. So one question to answer here is what should you do?

1. Wherever you must ensure that your users do not have local administrative rights.
2. If you want to control real equipment, the best solution is a third-party solution for companies like SecureWave, GFI or ControlGuard, etc.
3. Make sure that device control is based on whitelists (including authorized devices) in place of blacklists (including unauthorized devices). This will reduce complexity, administrative burden and increase overall security.

In the next article we will look more closely at the above principles and will tell you why and how Windows Vista can handle device control, which compares with Windows XP and Windows Server 2003.