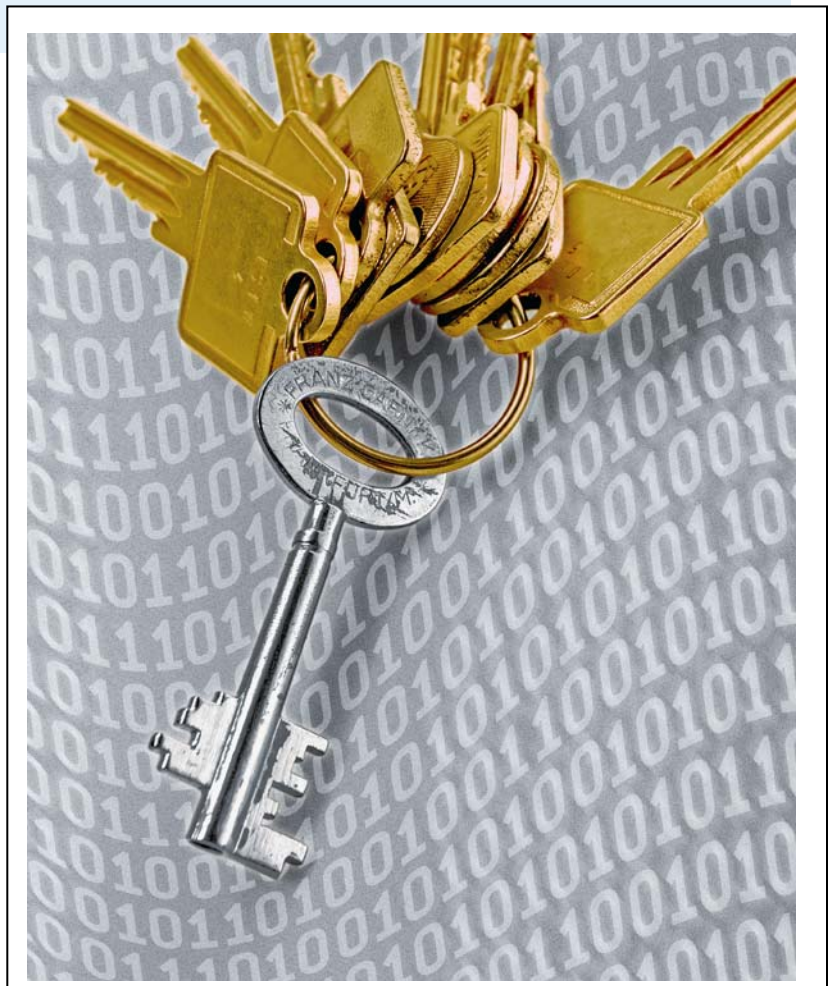




Device Control in Windows Vista

Why Vista is not enough



|

Device Control in Windows Vista

Why Vista is not enough

Introduction

Microsoft Windows Vista represents a big advance in the Windows family of operating systems. While many of Vista's features will help organizations with administering and securing their network environment, its new features for implementing control over the usage of removable devices will not be sufficient for most organizations. Vista implementers will find that Vista's limited control does not meet their needs and is too difficult and time-consuming to configure. For effective device control, organizations will still need to depend on third-party solutions, such as CenterTools DriveLock™.

Identifying Shortcomings

Microsoft has published a Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy at <http://www.microsoft.com/technet/windowsvista/library/9fe5bf05-a4a9-44e2-a0c3-b4b4eaaa37f3.mspx>.

The following table explains the shortcomings of Vista's approach by looking at each of the scenarios covered in Microsoft's guide and by comparing how administrators can use DriveLock™ to achieve the desired functionality easier and in a more meaningful way. The table also lists a number of DriveLock™ benefits that can't be accomplished at all by using Windows Vista alone.

Scenario	What Vista Does	What DriveLock™ Does
Configure policy to prevent installation of any device.	Vista enables this type of control. However, any device that was installed before the policy was applied is not affected.	DriveLock™ allows administrators to control the use of devices, not only the installation. Administrators can have separate policies for different device classes, for example, allowing the use of USB-connected mice or keyboards, while preventing the use of unauthorized network adapters or storage devices.

Scenario	What Vista Does	What DriveLock™ Does
<p>Configure policy to allow administrators to override device installation restrictions</p>	<p>Vista can enforce this effectively, but the Administrators group is the only group for which an exemption can be defined. After an administrator uses a device, including a USB stick, this device can be used by anyone unless the administrator uninstalls the device.</p>	<p>DriveLock™ allows usage exemptions for any group or user. Furthermore, DriveLock™ enables user and group-specific permissions for the use of specific devices. For example, DriveLock™ may allow help desk personnel to use a USB flash drive but not allow regular users to access these devices.</p>
<p>Allow users to install only authorized devices</p>	<p>Requires administrators to manually create a list of allowed devices by installing them on a computer, recording hardware settings for each device, and then copying these settings into a GPO. This is not practical in an environment where multiple computer configurations are in use. Devices can only be controlled by model, but not based on device type or a specific serial number.</p>	<p>DriveLock™ can scan computers for installed devices and then allows administrators to use this data to create white list policies. Administrators normally don't have to track down hardware identifiers of each allowed device. More important, DriveLock™ can allow or deny access to entire device classes or allow access to a unique device based on its serial number.</p>
<p>Prevent installation of prohibited devices.</p>	<p>Vista can accomplish this, but excluding specific devices from a network is not a common scenario and is not practical. Devices that have already been installed can't be controlled.</p>	<p>As with rules that allow access, DriveLock™ can block access by device class, device serial number and user or group. Blocking takes effect even for devices that were installed before the policy is applied. Device information about prohibited drives can be collected from the Device Scanner database, so an administrator doesn't need to install the device on a computer and manually record the device information.</p>
<p>Control read and write permissions for removable media</p>	<p>Only allows administrators to allow or deny all access to several types of removable devices.</p>	<p>DriveLock™ recognizes more types of devices and provides more granular control. Read or Write access can be controlled based on user, file type or even a specific device.</p>

Scenario	What Vista Does	What DriveLock™ Does
Auditing of device usage	Vista can't do this	DriveLock™'s Device Scanner, Security Reporting Center and file shadowing capabilities satisfy the needs of most organizations for auditing device usage and collecting forensic evidence.
Encryption of mobile data	Vista can't do this	DriveLock™ can transparently encrypt all data copied to and from USB flash drives and other removable devices. DriveLock™ can also enforce that only encrypted devices can be used on a computer.
Temporary unlocking of devices to enable exceptions	Vista can't do this	DriveLock™ enables online and offline unlocking of devices for a fixed period of time. This enables help desk personnel to respond in situations where legitimate access to removable devices is needed even if the currently active policy denies this access.

Scenarios Not Supported By Vista

The following list contains just a few examples of common device control requirements that DriveLock™ can easily enable, but that are impossible or impractical to configure with Windows Vista:

- » All users may use any USB-connected mouse or keyboard, but not removable storage devices.
- » Only administrators and help desk personnel are allowed to use removable storage devices.
- » No executable files may be copied from removable media to a corporate computer, except by administrators.
- » All data copied to USB flash drives must be encrypted.
- » Administrators need to be alerted when a user uses a removable device contrary to company policy.

- » Help desk personnel must be able to let a remote user copy a file to a USB flash drive even when the current policy normally prevents this.
- » Users should only be allowed to use company-issued USB flash drives.
- » Users should be allowed to listen to music CDs but they may not access CDs that contain data.

Conclusion

Organizations that are very small or have an extremely limited hardware base may find that Windows Vista is sufficient for controlling device usage. However, CenterTools believes that Windows Vista does not address the device control and security requirements of the vast majority of companies and organizations. Furthermore, when using the features built into Windows Vista, granular device control requires an inordinate amount of administrative resources. Organizations that migrate to Vista will find that additional software is required to provide effective and meaningful control of mobile devices.

DriveLock™ provides granular and comprehensive device control. It is easy to implement, easy to administer and easy to use.

To read more about DriveLock™ or to download a fully functional trial, visit www.drivelock.com. You can also contact CenterTools by calling (888) 627-7515 or by sending e-mail to info@centertools.com.

DriveLock
Intelligent control of mobile devices