DeviceGuard

The software solution for secure interfaces

DeviceGuard – The software solution for secure interfaces

Overview

DeviceGuard is a tool for monitoring and administration of:

- *logical drives,*
- *USB- devices,*
- *parallel and serial ports,*
- *FireWire- and infrared ports,*
- *WLAN devices.*

In the age of memory sticks, USB hard disks, FireWire hard disks and digital cameras data media handling becomes more flexible, but data security is frequently neglected thereby.

DeviceGuard can monitor drives, USB devices, parallel and serial Ports, FireWire, Infrared ports and WLAN devices and dynamically controls the access to these devices on computer and/or user level.

A practical solution

Logical drives

DeviceGuard permanently monitors the drives, which are available on user's computer. The decision whether a drive is provided on the computer depends on drive type (Floppy, Removable Drive, CD/DVD/CD-RW).

When a drive type is detected which is not allowed on the computer the access to this drive is locked. Additionally the locked device can be hid.

USB port monitoring

DeviceGuard can monitor connected devices. The USB device identification takes place on base of VID (vendor ID) and PID (product ID) values. To monitor a specific device the exact VID/PID value is entered in the monitoring list. Furthermore monitoring of USB device classes is possible. So for example input devices (HID – Human Input Devices) can be allowed and USB drives (USBStor) can be locked.

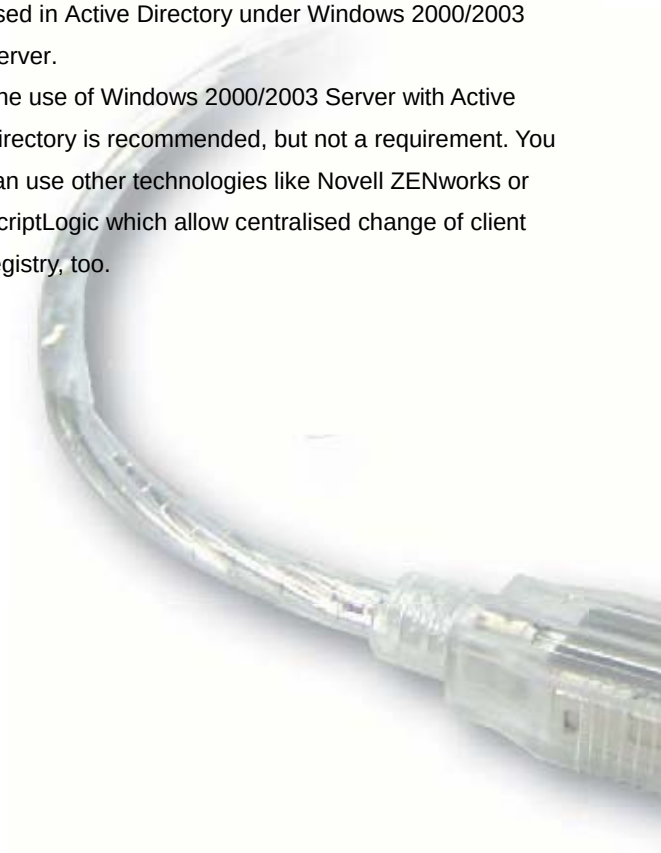
Parallel, serial, FireWire, infrared, WLAN ports

DeviceGuard can monitor parallel, serial, FireWire, infrared and WLAN ports and control the access dependent on user and computer according to the central configuration.

Administration of DeviceGuard

DeviceGuard is configured via the registry of the computer which runs DeviceGuard. For central configuration of all computers in a network a policy template (deviceguard.adm) is provided which can be used in Active Directory under Windows 2000/2003 Server.

The use of Windows 2000/2003 Server with Active Directory is recommended, but not a requirement. You can use other technologies like Novell ZENworks or ScriptLogic which allow centralised change of client registry, too.



Logging

DeviceGuard logs it's activities to file or send SMTP messages if activated. SMTP messages will be sent, if prohibited devices are connected to the client PC. To protect users anonymity, all user information can be eliminated during logging and SMTP messages.

Installation

DeviceGuard is installed as a service on a client computer using the MSI package *DeviceGuard.msi*. DeviceGuard service installation can be done using Active Directory software deployment solution or any other software deployment solution.

Security

Users and power users cannot close DeviceGuard or end any of its processes (tasks) – this can only be done by administrators. This ensures that there is no way of bypassing or cancelling the device restrictions. What's more, users and power-users cannot delete DeviceGuard program files.

System requirements

- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista (beta).

DeviceGuard is administrated by group policies in *Microsoft Active Directory* or *Novell ZENworks*. DeviceGuard Monitor requires Microsoft .NET Framework 1.1.

contact

e-mail: info.kilonca.de
website: www.kilonca.de