itWatch

GmbH

itWatch GmbH ✗ Aschauer Str. 30 ✗ D 81549 Munich

Devices out of control

Effectively combat plug&play security deficits in Windows 2000 and XP

SioS GmbH, a management consulting company for IT security (www.SioS-GmbH.de) has been pursuing for some years a welcome change in the market for IT security for Microsoft clients. IT security has a reputation as an eternal disabler of innovation. Therefore DeviceWatch (www.itWatch.info) is an outperforming innovation. DeviceWatch is a security product which is used even in environments with increased security requirement (items of classified information) in the military sector. In addition to the security function it offers significant added value for the system management and as a result interesting cost savings.

The uncontrolled usage of plug&play devices has been identified in many instances as a threat - unfortunately often after the damage has already been done. From the viewpoint of company management there exists a significant requirement for action, as is well known to the security officer of a trading holding with 20,000 PC's.

In an ongoing survey being conducted by SioS GmbH, security officers from more than 1000 companies have been asked how they are tackling these new challenges. The number of workplaces in the companies varied between 100 and 400,000. In most cases the persons interviewed are fully aware of the problem. The most frequent countermeasure consists in bookish instructions, whose unsuitability is well known. Delays in projects result, since either no solution to the problem is yet known or the effective management of the existing variety of devices is approached with trepidation because of the high item numbers. The roll-out of new Windows environments, however,

sets standards in companies and it is very difficult to later implement restrictions or new release processes if everything has been allowed at the beginning.

DeviceWatch allows the user, group and machine-related approval of separate devices in a network by means of a central administration. The functions a device offers may even be administered individually if desired. Thus printing on a multifunctional printer can be authorized for all users, however, scanning, faxing, data extension using memory sticks and the modem function can be limited to individual users or groups in each case. The chief security officer of a German building and loan association determines that his decision in favor of DeviceWatch, following a careful market analysis, was made because the complexity of the security policy will grow with his requirements and a roll-out covering all his needs was possible in only two days. Picture 1 shows how easy it is to build, understand and maintain a security policy.

DeviceWatch can be integrated into all infrastructures without the

Picture 1: Definition of a security policy
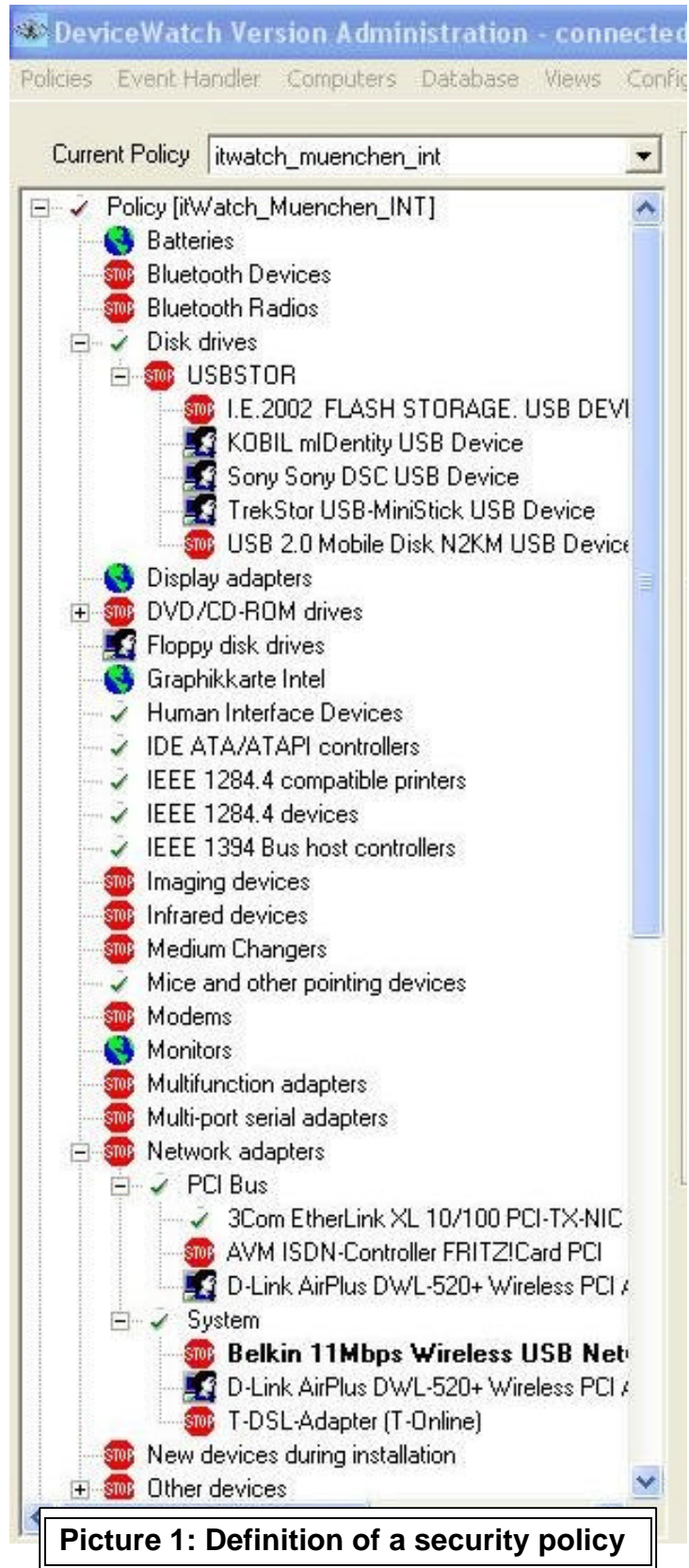
customer having to change his processes. Rather, DeviceWatch adapts itself to customer processes and even allows the customer to organize the flow of information for the procurement. The application form required for the process is referenced in the product and any approval procedure is supported by DeviceWatch. DeviceWatch finally convinced the Chief Security Officer at a state bank with more than 10,000 computers through the life cycle management of the security policies: "Before importing a security policy in our productive environment we have to perform a strict process using our test bed up to the point of approval through the different parties responsible, including subsequent import into the productive environment. All these functions and those required for auditors and archiving are already included in the product."

As well as these functions, DeviceWatch offers further added values, which form the bridge between security and system management. DeviceWatch Scanner registers the entire inventory of mobile and inbuilt devices. Not only those devices are identified being connected when a scan is executed, but also all those devices are reliably identified and reported which were at some time in the past connected to the workplace - also in off-line operation. In this way high-quality and permanently updated interfaces are provided for inventory and asset management.

The function of DeviceWatch DEvCon is brand-new. DeviceWatch DEvCon enables the setting of conditions for decentralized actions on the PC in the central administration environment. The action can be any arbitrary program or script or a pre-assembled DeviceWatch module. Three pre-assembled DeviceWatch modules are delivered
- signaling the event to a central event console
- the execution of self-generated scripts
- the automated assigning of disk-drive letters to mobile disk drives

The diverse operational scenarios of mobile devices causes increased Help Desk calls. This leads on both sides – that of the user and that of the it-operation e.g. call center - to a dissatisfaction with modern technology. Error resistance, security, especially integrity, of the PC and user friendliness have to be guaranteed to satisfy all parties. This area of conflict is solved with DeviceWatch. A basic requirement for many areas of application in the medical sector is e.g. the secure integration of PDA's in the network. Automatic synchronization of PDAs without any user interaction is pragmatically solvable. Incidentally, it can also be ensured that the PDA is in fact one of those belonging to

the company. Picture 2 shows an example how to achieve this using DeviceWatch.

Picture 2: Controlling PDA synchronisation using central administration
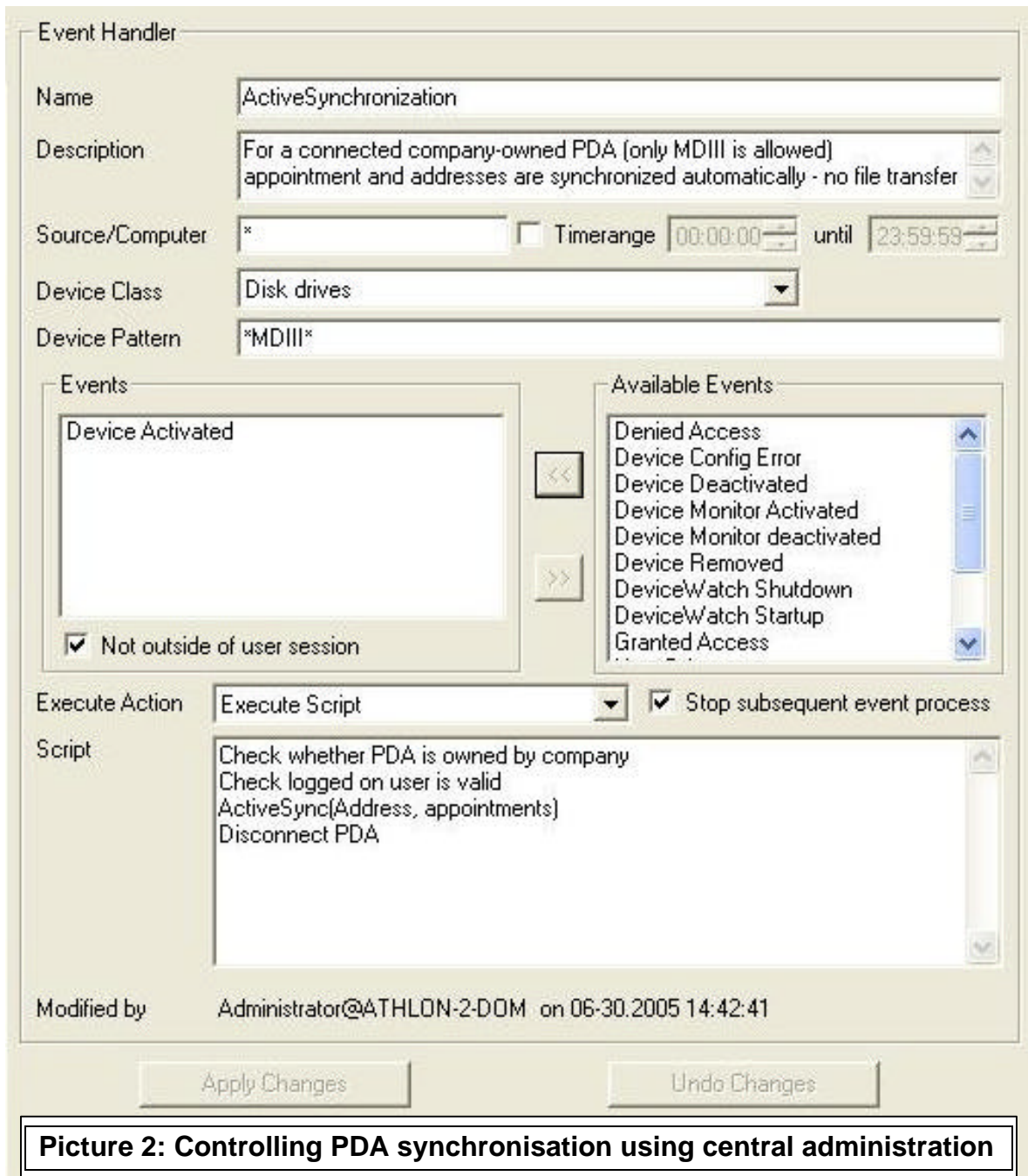
In this way DeviceWatch helps the customer, even in times of high pressure on costs and tight budgets, to utilize important resources optimally and to operate IT systems in a low-cost way, as Mr. Maier, CEO of StarTech is pleased to report. Because only those companies who keep their IT under a cost-optimized control are competitive and successful in the long term.

The IT manager of the SANA clinical center justifies his decision in favor of DeviceWatch as follows: "The product scales perfectly, so that we could begin in a small way and can extend the installation as required in a simple and low-cost manner. The personnel expenses are very low, since we required no external consultation or manufacturer support in order to bring the product into the production. DeviceWatch is so simple to operate that we could start without training. For those few questions which arose before the introduction, we got competent and efficient answers from the hotline of itWatch (www.itWatch.info). This innovation from Germany is highly recommended by us."

The IT service provider of one of the largest European insurance companies found not only the technical added value for his customers to be attractive, but in particular the low operating costs. Being responsible for 120,000 PC`s he summarizes the company requirements in the environment of secure device management:

"Every PC user who has access to the modern interfaces of a PC (USB, Firewire, Bluetooth, WLAN, PCMCIA, Infrared etc.) can use a great number of devices without the data-protection laws or in-house requirements being capable of being technically applied. Mobile devices, such as cameras, memory sticks, DVD burners and other external data storage media are, however, fixed component parts of the present business processes, since they minimize overall costs. However, we cannot afford to turn a blind eye to the uncontrolled usage of such devices and, after ongoing market analyses which took 14 months with extensive testing, we decided in favor of DeviceWatch - after one year of productive deployment we would make the same decision again today".