HP PROTECTTOOLS DEVICE ACCESS MANAGER

Business white paper

A fundamental requirement of securing a computer system is the control of the import and export of data and executable code. With data, the major issue is the theft of electronic data and consequential loss of intellectual property and proprietary information. In certain organisations such as financial institutions and government bodies, the sensitivity of the information is obvious. However, it is important that all organisations provide adequate protection and in many situations this is a legal requirement.

The threat with executable code is different; the major concern here is the introduction of Viruses, Trojans and other illicit software. These present potential security issues. The risks with Viruses and Trojans are clear but, enabling users to install and use unauthorised software comes with a new set of risks. Users may expose the organisation to licensing problems, deviate from the "standard" application set and create non-standard data sets, all this will increase support and maintenance costs. When you add to this the problems associated with games and other inappropriate software it's easy to see how any organisation can benefit from controlling the import and export of data and executable code.

Risks

Removable Media
USB, Bluetooth, Compact Flash
Unauthorised Software

The hazards presented by CD/DVD drives and floppy disk drives have been understood for some time but, we are now faced with a vast array of devices that can be easily obtained and are automatically recognised by Windows systems. Drivers are installed, often without the need for any administrative privileges. The existing parallel and serial ports and other expansion capabilities offer opportunities to connect an assortment of plug and play devices. These devices include USB memory sticks, other external storage devices (Compact Flash, SD/MMC, Hard Disks), scanners, digital cameras and other PDAs.

In many cases these devices are essential for carrying out day-to-day business but they are all a security threat. One option is to have devices removed from the system altogether but this is expensive and results in non-standard system support and creates maintenance problems. One of the principal concerns is USB ports, and with more computer systems shipping without legacy port support, the USB port must be left enabled to support even the mouse and keyboard.

There are of course devices that present specific threats but which do not allow data to be stored, good examples of these are Bluetooth modules and Wireless networking plug in cards. These devices are readily available and easy to install allowing wireless connections. Whilst these can have benefits the unauthorised adoption of such devices can lead to serious security risks extending the corporate network in an unmanaged way.

Device Access Control

HP ProtectTools Device Manager controls the access to all of these devices based on the user's permissions. It can even control the type of devices users can connect to a particular port. For example, a user with permissions can connect a particular printer, mouse and keyboard via a USB port whilst excluding any mass storage device or Bluetooth module. These permissions apply when the device is present as the user logs in or if the device is hot plugged into the logged on running system.

Permissions on devices may be set with individual

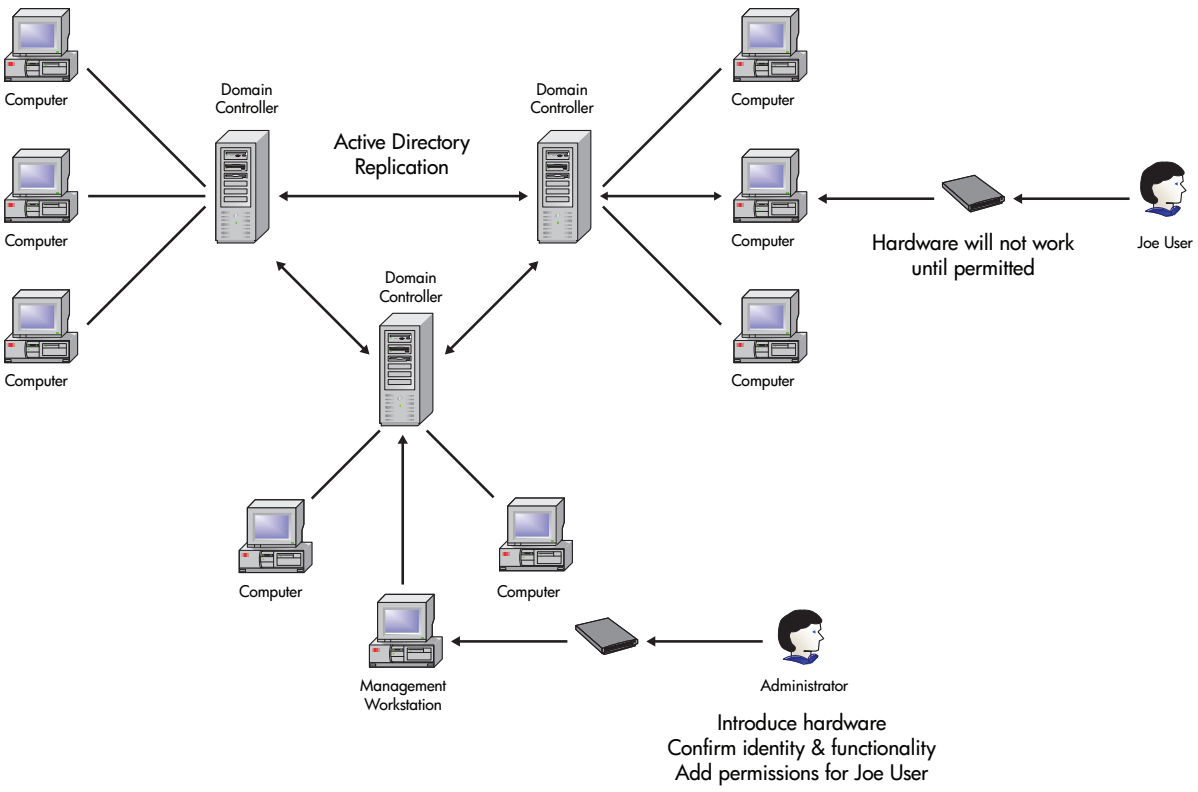

Figure 1. *Access Control Replication*

device granularity on a user or group basis. Control of these permissions is through an extension to "Active Directory Users and Computers", an extra tab allows devices recognised on the management workstation to be moved to the permitted devices "White List" for an individual user or group. Devices not moved to the "White List" will not be available to the users. This configuration data is stored in the Active Directory integrating with the standard configuration propagating around the domain in the normal way. This design avoids the need for a separate configuration data store.

When the user logs on the configuration data is retrieved from the Active Directory and cached locally, this cache is updated at regular configurable intervals. The principal advantage of this cache is that it allows device access decision to be made without reference to the central data store, it also allows off line working, for example with laptops disconnected from the network.

Devices that can be controlled include USB, PCMCIA, Infrared, Bluetooth, Modems, Serial/ Parallel ports, IEEE 1394 Bust host controllers and other removable disk drives. There is a set of devices which are not viewed as a security threat which by default are enabled. These include devices such as Keyboards, Mice, Graphics Controllers and Smart Card readers.

Active Directory Configuration
Device White list
User and Group Based Configuration

The access control policy can be reviewed from the management tool either by user or by device. It is possible to see which devices a particular user or group can access or to list the users and groups who can access a device.

By controlling device access through groups in the configuration, all users who need access to each device can be added to the domain group of that device. Of course, the configuration for several devices for a category of users can be associated with a group so that when a new user joins a team they can be simply added to the group and pickup the device permissions they need to do their job.

As the device permissions are controlled centrally, it's a very simple process to grant temporary access to a device by adding the permission into Active Directory with no need to visit the workstation.

CD Auditing

It is increasingly common for users to need access to CDs for directories, manuals, etc. In these situations locking the device is not appropriate, instead an audit trail is required.

HP ProtectTools Device Manager allows auditing of CDs inserted into, and removed from, the CD drive. This feature uses the Windows Event log and records the CD label, user, date/time and whether the CD is being inserted into, or being removed from, the drive. So when a user is trusted to use the CD drive an audit trail is available to ensure the device is being used only for legitimate purposes.

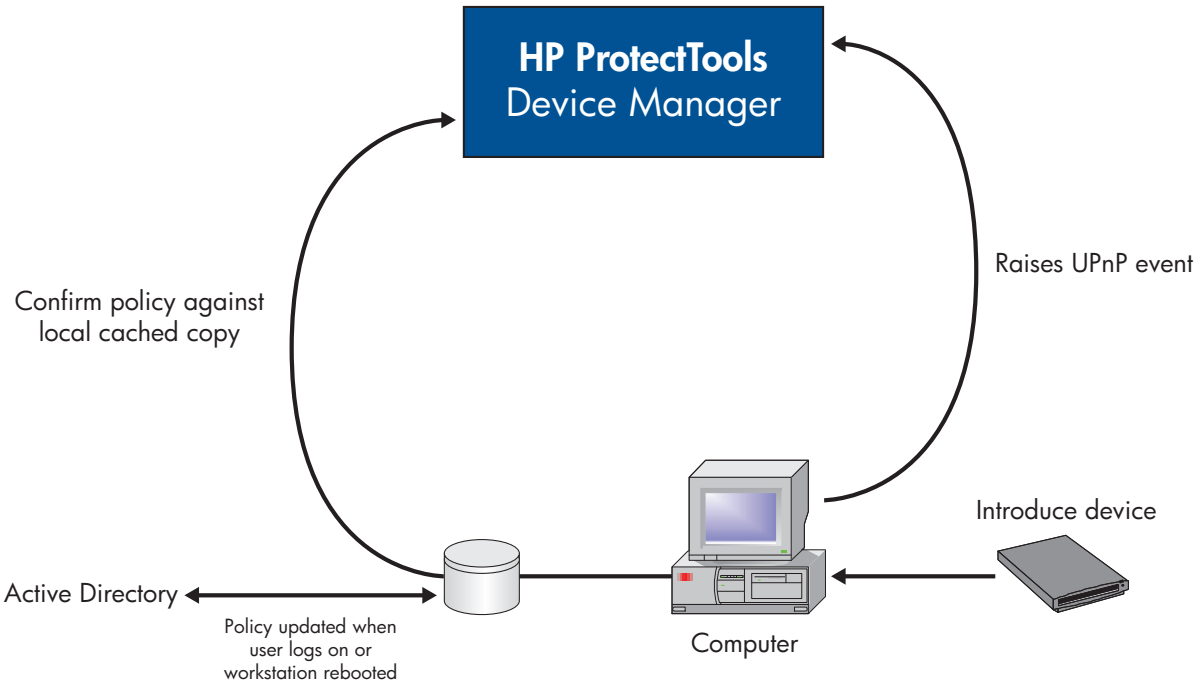

Figure 2. *Device Access Caching*

File Type Access Control

In many circumstances the day to day business requires access to removable media, in this situation it is necessary to allow access to the type of files the user needs to carry out their work but preventing access to unauthorised files. For example, users may need to be allowed to work with Word Documents but prevented from accessing MPEG files.

Strong Auditing

User
Devices
Files
Workstations

In addition to controlling which devices can be used to transfer data to and from a workstation, HP ProtectTools Device Manager can restrict which file types can be transferred. Lists of permitted file types, identified by their extension, can be controlled for each user or group. These permitted file types are configured through the same Active Directory management tool and managed in much the same way. Registered file types are listed and those which the user or group has permission to transfer are selected. Permissions can also be set for unregistered file types based on their extension.

File Auditing

As well as limiting access only to particular file types it may be desirable to limit the operations to be carried out. Whilst there are good reasons to allow files to be copied to and from the removable media there are other operations such as executing a program from the removable media that are much less desirable from a security perspective. These extra privileges to access removable media come with a requirement for additional monitoring; the normal mechanism for providing this is enhanced auditing.

HP ProtectTools Device Manager provides an additional interface that limits operations to the copying of files to and from the removable media; users are prevented from running programs directly from the media. The HP ProtectTools File Explorer component allows auditing of files copied to and from removable media. This feature uses the Windows Event log to record the file names, destination directories, user and date/time. Users can therefore be given a limited level of trust to use the removable media for legitimate purposes with an audit trail available should it become necessary to trace an individual program or file.

Conclusion

Securing company data is becoming a vital issue in a workplace where an increasing number of devices can be used to import and export data from company networks. All types of businesses and organisations can use HP ProtectTools Device Manager to regain control and manage these devices effectively. The management and auditing tools available in this software allow organisations to operate with flexibility whilst retaining a robust security policy which is easy to manage. Make sure your company data is secure with HP ProtectT ools Device Manager.

For more information

If you would like to try this software for yourself please visit our Software Depot website (www.software.hp.com) where you can download free 60-day evaluations.

www.hp.com/hps/security/products

HP ProtectTools Security Team, 2004

Call to action

www.hp.com/hps/security/products
email: protecttools@hp.com
Tel: +44 (0) 1925 841881.

4AA3-4641EEE, Created May 2011