CONTROL

HP ProtectTools Enterprise Device Access Manager

From the HP ProtectTools Portfolio

With the rise in mobile devices such as smart phones that are becoming as sophisticated as laptops and PCs, and devices that can easily move huge amounts of data like USB sticks and Bluetooth, it is important for organisations to control which devices their users can and cannot use on their company systems and networks.

Some devices not only facilitate the accidental or malicious loss of sensitive data but they can also corrupt your company's systems and networks by introducing Viruses, Trojans and other illicit software.

Protect your Reputation

The Information Commissioners Office (ICO) has the power to fine companies who breach the Data Protection Act and lose data. The ICO has not been shy in flexing its muscles and has handed out several fines reaching tens of thousands of pounds to organisations that have not protected their customers' information.

In 2010 an average data breach costs UK companies £71 per record or £1.9 million. This figure is up 13% from 2009[1].

Protect your IT Infrastructure

HP ProtectTools Enterprise Device Access Manager allows you to build a centralised control policy of devices within your organisation. By controlling which devices users can access you can prevent your IT environment being infected with malicious software. When users have the ability to install new applications from external media, such as music playing devices, it is much harder to control your IT estate and support and maintenance costs can escalate.

Managing Devices

A standard PC comes with a vast array of devices that are either pre-installed or easy to purchase and automatically recognised by Windows systems. These data storage devices such as memory sticks, pen drives and SD cards can be easily removed giving them a high risk factor in the loss of data.

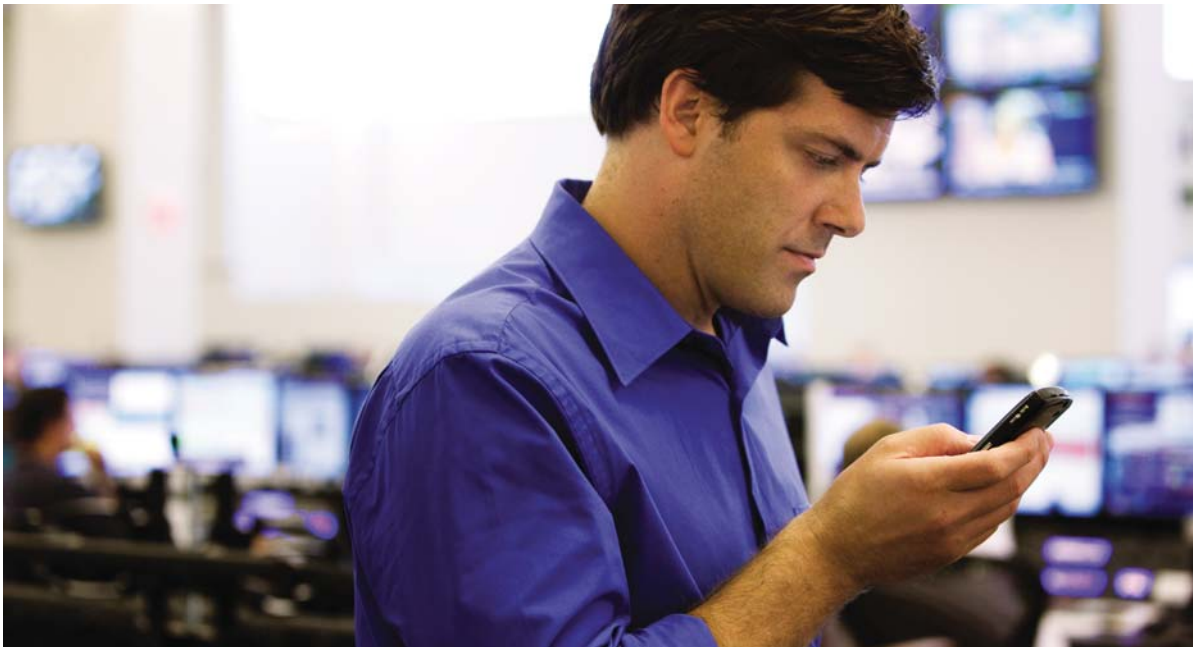
Devices that do not store data but extend your corporate network in an unmanaged way also pose a security risk. Examples of these devices are Bluetooth and Wi-Fi, which can bring malicious software into your network if not managed properly. HP ProtectTools Enterprise Device Access Manager is unique in its ability to block Wi-Fi and Bluetooth in the device blocking software marketplace.

Securing mobile devices continues to pose a challenge to business with 62 percent of respondents identifying this as a challenge[2].

During the day-to-day running of your business many of these devices will be essential but that does not reduce the threat to your data security that they present. With Enterprise Device Access Manager you can control devices across your entire organisation.

In 2010 over 17,000 USB sticks were left at the dry cleaners by mistake[3].

HP ProtectTools Enterprise Device Access Manager can either disable or force read-only on devices that can store and transfer large amounts of data such as USB Mass Storage Devices and CD/DVD drives. This prevents your organisation's sensitive data from being copied to these devices.



Key Features

- Centralised control of devices within your enterprise
- Read/Write control of Removable Disk Drives and CD/DVD Drives
- Control over devices that extend your corporate network, e.g. Bluetooth, Wi-Fi
- Management tool integrates into standard Windows management tools
- Several property pages catering for Administrators with varying levels of experience
- Utilises Active Directory to store and propagate the device access control policy to end-points within the organisation

Devices that are already installed on the PC as well as those that are added during the session can be controlled with Enterprise Device Access Manager. Every time a different user logs on to the PC the device access permissions will change dynamically.

In 2008 a memory stick was stolen from an unsecured office and walk-in clinic of the Chelsea and Westminster Hospital NHS Foundation Trust. The memory stick was not password protected. The device contained sensitive medical information for 143 patients. You need to manage what information can be transferred to portable devices such as memory sticks to ensure the sensitive data you hold remains safe[4].

Enterprise Wide Configuration

You want to be able to control mobile devices but don't want it to create masses of extra work for the IT team. HP ProtectTools Enterprise Device Access Manager is easy to set up and utilises existing Windows features and functionality. The management tool integrates into Active Directory Users and Computers so there is no need for additional hardware or software. The device access control policy can be set up using one of several property pages depending on the experience level of your system administrator.

System Requirements

- Active Directory
- Administrator Component: Microsoft Windows Server 2003 (32 and 64-bit), Microsoft Windows Server 2008 (32 and 64-bit), Microsoft Windows XP (requires admin pack)
- Client Component: Microsoft Windows XP (32-bit), Microsoft Windows Vista (32 and 64-bit), Microsoft Windows 7 (32 and 64-bit)

HP ProtectTools Enterprise Device Access Manager is part of the HP ProtectTools portfolio, for more information about the product and the other HP ProtectTools products please visit www.hp-protecttools.com or call 0800 03 80 710.

1 Symantec data breach survey 2010

2 Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency - McAfee Report 2010

3 Credant Technologies research

4 ICO notice of data breach http://www.ico.gov.uk/upload/documents/library/data_protection/notices/chelsea_and_westminster_undertaking.pdf

4AA3-5657EEE, Created June 2011