



This feature article outlines issues surrounding Microsoft *“Stealth Updates”*.

“Microsoft is now including Product Activation technology in several Microsoft products - To try to reduce software piracy and to make sure that all Microsoft customers receive the product quality that they expect.”

On the face of it this sounds a reasonable approach, but there are some real technological challenges that are introducing risk to your organization through “Stealth Updates and a widening of the approach through Software License Protection Services”

Stealth Updates, May be coming to a PC near you!

is a feature article, in the
Managing Clouds and Moving Goalposts ©
series of “Management Focused” articles
by **PCProfile** <http://www.pcprofile.com>

Introduction

For the last few weeks the IT press has been adrift with stories, editorial and user comments on Microsoft's Stealth Updates and so on after recent discoveries that nine (9) executable files were "silently updated" despite users having "turned off" auto-update features. see <http://www.windowssecrets.com/2007/09/13/01-Microsoft-updates-Windows-without-users-consent> and follow the user comments about their concerns about Microsoft's approach.

There is a trend emerging that end users need to be aware of relating to product activation under the Windows Genuine Advantage (WGA) program.

Microsoft plans to widen this approach further as "Software License Protection Services" and is offering this to all software vendors.

Our concern is that this will introduce significant risks that you hadn't planned on by allowing backdoor entry into your systems.

Microsoft has replied, in a fashion about the issue of "Stealth Updates", through their Technology Blog writers justifying the "silent update" requirement, however the consensus amongst the user community is that the end user needs to be TOLD beforehand so that "they can decide when to apply" and "whether they agree to any changes to system configuration files".

It's no good getting out the End User Licensing Agreement (EULA) and arguing the semantics of whether Microsoft can or can't do this. This is a fundamental security issue that needs wider consideration.

Why? IT Managers and CIOs already have an ingrained fear of attack vector approaches by software vendors and malicious sites who cotton-on to the idea that it's OK to silently install software to systems.

Most IT Managers at large sites have sophisticated monitoring tools that are set to watch and detect suspicious activity and have already wasted many hours poring over large audit and log files looking for intrusion attacks on their systems only to find that the files changed, 9 executables, came via Microsoft. This was despite having Automatic Updates (an embedded feature in Windows) turned off.

Now its time to widen the perspective and look at a wider range of issues looming that will impact management of business systems very soon.

You could be cynical and take this view -

Microsoft Stealth Updates



"Hi, this is Bill Gates. Time to buy some new software."

**WGA
Ambushes
Innocent
victims**

Windows Genuine Advantage, Microsofts' anti-piracy Software Protection Platform, has already delivered "no advantages to a whole bunch of users" recently. See <http://www.gripe2ed.com/scoop/story/2007/9/17/0944/52635>

The recent debacle, which Microsoft promptly resolved and supported, had some end user sites ambushed as "pirates" when they connected to the Internet and Microsoft activation servers "detected license anomalies" that degraded the performance of their systems.

Those users that had proof that they had legitimately purchased, installed and previously validated XP and Vista systems were able to, with phone and email assistance from Microsoft, to eventually validate and reset their systems so they could get back online and continue business operations. See what happens when your system is presented with an error message of "Your activation period has expired" <http://support.microsoft.com/default.aspx?scid=kb;EN-US;925616> and "The behavior of reduced functionality mode in Windows Vista" <http://support.microsoft.com/kb/925582/>

Reduced Functionality means that some experienced disruption to business operations and this would cause unexpected grief for end users and their customers relying heavily on systems being online for point of sale, e-commerce, trading and business activities.

These sites, due to the processes used by Microsoft for validating their systems, had their licenses deactivated and they were forced to re-activate again, through a hock-up in the Microsoft activation server rooms of a server side deployment of non-approved software.

We have since learned later that "human error" (lack of configuration control?) is the bottom line issue here which caused Microsoft activation servers to reject access to software until such time as the end user activated it via online or via phone call.

For more information see <http://blogs.msdn.com/wga/> and <http://windowsvistablog.com/blogs/windowsvista/archive/2007/08/25/addressing-wga-validation-issues.aspx>

**Activation
Methods**

Activation is an integral part of the Windows Genuine Advantage (WGA) and its child "Office Genuine Advantage" (OGA).

We presume that Microsoft Activation will spread to other products in the form of;

- VGA (Visio Genuine Advantage),
- ProGA (MS Project), and

a myriad of other Microsoft Applications - that will all be touting the Genuine Advantage of registering the software and activation by web interfaces.

Microsoft Software Protection Platform, is an anti-piracy initiative designed to protect Windows Vista from illegal copying and license tampering. See <http://www.microsoft.com/presspass/features/2006/oct06/10-04SoftwareProtection.msp> and <http://www.microsoft.com/presspass/download/features/2006/10-03-06SoftwareProtectionWP.doc> (.doc file, 2.7 MB)

**PCProfile's
View
On
Activation.**

PCProfile has been active as an adviser to businesses in terms of anti-piracy protection since 1991 and understands the reasons why Microsoft have gone down the path of activation.

The concept of engaging activation through dialing/connection via the Internet back into an activation server at Microsofts' offices at Redmond (or wherever they have the system located) is to limit the spread of license keys being duplicated, hacked, generated, given away, or sold off for a token fee, when in fact only a defined number of valid serial numbers exists and was released/purchased in the 1st instance.

PCProfile has no problem with the notion of activating software ONCE ONLY as a

means to validate that only one (1) software license is applied per seat to a system to minimize the effect of piracy and to do this some generic data needs to be gathered on a point-to-point Internet connection basis.

But PCProfile, like many others do have some concerns over the data collected (even if it's encrypted) by Microsoft, particularly with the security over the data as it is transmitted via open ports on your PC and to arrive at its destination (Microsoft's Redmond servers) it needs to travel via a number of servers and sites via data hops.

The real problem lies in the fact that in applying these digital techniques of activation and validation through Digital Rights Management (DRM) approaches, is that the advantages are being lost to the end user business sites through the methods of deployment by Microsoft.

Don't forget that the end user business sites are the Microsoft customers who keep them alive with funding through license revenues but maybe Microsoft is losing sight of this?

**Description of
Microsoft
Product
Activation**

In Microsoft's own words - *"WPA ties your Product Key and Product ID to your computer by creating an installation ID. The installation ID is made up of your Product Identification (PID) and a computer identifier, called a hardware ID, or HWID. The installation ID is sent to a Microsoft license clearinghouse, which verifies whether Microsoft manufactured that PID and that the PID has not been used to install the operating system on more hardware than is defined by the product's License Terms. For Windows Vista, the License Terms state that you can install on one computer. If this check fails, activation of Windows Vista fails. If this check passes, your computer receives a confirmation ID that activates your computer. After Windows is activated, you never need to perform Product Activation again, unless you significantly overhaul the hardware in your computer. You must activate your installation within 30 days after installing Windows Vista.*

If the Product Key is used to install Windows Vista on a second computer, the activation fails. Additionally, if WPA detects that the current installation of Windows Vista is running on a different computer than it was originally activated on, you must activate it again. In this way, WPA prevents casual copying of Windows Vista."

**What is
Activation?**

Activation is an exchange of two mathematically computed codes between your computer and Microsoft that authorizes Microsoft software to run on your PC. There are five main components to activation:

Product Code

The OS contains the product code, which is installed on your HDD when you install the OS. Product codes are different for Windows XP Home Edition, Windows XP Pro, OEM licenses and volume licenses. They are not interchangeable. A Product Code is not a Product Key.

Product ID (PID)

The PID is generated by combining the Product Key that was supplied with your XP with the Product Code stored by the OS.

Hardware ID (HWID)

The HWID is generated by interrogating various hardware components on the computer. The values and codes that make up the HWID are based on serial numbers, volume IDs from hard disks and NIC MAC addresses (network cards).

Installation Identifier (IID)

The IID is a code that represents your OS installation and is made up of the HWID and the PID. The installation ID does not contain any personally identifiable information. It contains only a code that can be decoded to verify the components that make up the HWID.

Confirmation Identifier

The activation software sends the IID to what Microsoft call a clearinghouse. It is a Windows server running Microsoft Windows 2000 Advanced Server, Microsoft Internet Information Server, Microsoft SQL Server and Microsoft Certificate Server. The clearinghouse takes the Installation ID and sends back a Confirmation Identifier (CID), which contains the digitally signed license number that activates XP. This license number can be decoded into the PID, HWID, IID and the Product Key.

This link was recently updated by Microsoft to outline what activation is and why it is used. See <http://support.microsoft.com/kb/302806>

“Microsoft is now including Product Activation technology in several Microsoft products - To try to reduce software piracy and to make sure that all Microsoft customers receive the product quality that they expect.”

Activation uses a voting mechanism. There are 10 hardware characteristics used in creating the HWID:

- Display Adapter
- SCSI Adapter
- IDE Adapter
- Network Adapter MAC Address
- RAM Amount Range (i.e. 0-64mb, 64-128mb, etc)
- Processor Type
- Processor Serial Number
- Hard Drive Device Type
- Hard Drive Volume Serial Number
- CD-ROM/CD-RW/DVD-ROM

Activation Woes Are Not New

Microsoft's Activation server went offline in October 2006 causing disruption to licenses for XP users - see

<http://blogs.msdn.com/wga/archive/tags/outage/default.aspx>

The community forum at

<http://forums.microsoft.com/genuine/showforum.aspx?forumid=1004&siteid=25&sb=0&d=1&at=7&ft=11&tf=0&pageid=0> shows a large number of users experiencing all sorts of issues with validation of Vista and XP.

Adobe had similar problems with their own “Adobe License Manager (ALM) that was re-released in November 2006 and then was withdrawn in March 2007 due to the deployment issues that end user sites experienced with Adobe's approach to license management, which was also aimed at limiting piracy as well, as selling the benefits of “the end user being able to manage licenses easier”.

Ed Foster in his Gripe Log wrote about the issues of ALM in September 2006 at this link. “Adobe License Manager and Acrobat”

<http://www.gripe2ed.com/scoop/story/2006/9/25/01627/6990>

Activation woes are not new and are not just confined to Microsoft!

Adobe License Manager

For illustration purposes the following details are acknowledged as Copyright © 2007 Adobe Systems Incorporated, portions are listed here for clarity of this feature article.

Adobe License Manager Overview - extract from <http://www.adobe.com/support/products/alm.html>

Adobe License Manager (ALM) software automates the tracking of Adobe desktop software licenses and enables businesses to proactively manage and administer volume product licenses while minimizing the resource and cost burden associated with manual license management.

Extract from

<http://www.adobe.com/elicensing/licensemanagement/alm/>

Electronic licensing in Adobe products — Important changes

"In November 2006, Adobe introduced the Adobe License Manager (ALM) solution to automate the complex, labor-intensive, and confusing process of managing volume software licenses. Unlike traditional software asset management solutions that track files on computer hard drives, ALM was designed to manage the licensing entitlement through an e-license. A key element of this solution was a choice of where to host pools of e-licenses (either at Adobe or in-house), and customers have had the option to disable ALM altogether.

ALM was rolled out in Adobe® Acrobat® 8 for Windows to our volume license customers worldwide. However, during the subsequent three months, **we have learned that ALM requires a greater level of administrator resources than many of our customers have available to them. In some instances, there have also been difficulties in managing certain customer workflows and requirements.**

As a result, we have decided to disable the ALM technology in Acrobat 8 for all new volume license copies sold after March 9, 2007. Effective immediately, all Acrobat 8 for Windows installation media will be provided with ALM disabled. The final date for availability of ALM-related processes on the Adobe Licensing Website is April 9, 2007.

We plan to make significant policy, program, and technology improvements and reintroduce an electronic license management solution when it is robust and flexible enough to meet a broader set of our customers' expectations. **This reintroduction will occur in future versions of Adobe's key desktop applications to be released after calendar year 2007."**

For more information there are a further 25 FAQs to peruse at; <http://www.adobe.com/elicensing/licensemanagement/alm/faq/>

**Activation
and
Validation
Is
Planned
To
Spread
Wider!**

Microsoft at it's Worldwide Partner conference in Denver in July 2007 announced that from October 2007 Independent Software Vendors (ISVs) will be able to license, using similar techniques to WGA/OGA/DRM a new service called "Software Licensing and Protection Services" (SLP Services).

Microsoft Announces SLP Services to Streamline Software Development and Sales
The following information has been extracted from
<http://www.microsoft.com/presspass/features/2007/jul07/07-10slpservices.msp>

Thomas Lindeman, Microsoft group product manager, discussed ways in which Microsoft was going to offer and license source code to "help software developers protect intellectual property, manage licenses and increase sales through innovative business models". Read some of the selected quotations from the above link.

"As far as licensing enforcement, sometimes we call it "positive control," which means that what you intend your end users to do is all they can do, and the Secure Virtual Machine (a piece of code called a Secure Virtual Machine (SVM) now resides inside the application) handles this protection and management as well. So there is a client-side license enforcement process that makes it down to the end user, and then the licensing component of the code protection software looks at that license and controls the application in whatever way the license states. It basically enforces the license's rules."

"Another main feature that Code Protector SDK with SVM performs is to allow the ISV to mark different functions and features as licensable and monitorable entities. That means when the ISV's business or product-marketing group wants to create digital licenses for certain feature bundles, or SKUs, they can easily turn on and off those features that were marked as protected and deliver only the desired functionality to the end-user."

"They can also gather the monitoring data, which can be used for things like billing, such as utility based billing at the end of the month, or to create statistics on what usage has happened within the application for future product planning. Application monitoring is an optional feature, and we expect the ISV to allow the end-user to opt in to such a process."

"An important point here is that the code is separated from the digital licenses that control it, and they do not need to be created or finished at the same time in the product cycle. This enables what we call "SKU agility" — the ability to fine tune software offerings even after the product has been shipped. "

"..... being able to target customers in a direct way, where you're giving them exactly what they need and only what they need. You can think of a utility-based model where they're only using the features or functions or amount of time that they want, and you can bill them after the fact. Customers could pick and choose a certain number features that they want to use, get a use license, and only pay for those features."

**Now, start extrapolating issues with
Activation across EVERY software
application you trial, license, install
on your systems!**

What is the impact going to be?

**Software
Licensing and
Protection
Services
(SLP Services)**

Key elements extracted from the press release for Software Developers (ISVs) are;

- Code Protector SDK
 - to help third-party ISVs control and manage their intellectual property, as well as manage sales and licensing processes.
 - licensing and activation of native code applications will be available with the first release
 - mark features as "licensable entities" that can later be controlled through various kinds of digital licenses, as well as providing client-side protection of those licenses.
- Software Licensing and Protection Server, in standard and enterprise editions.
 - allows the ISV to host their own servers,
 - create licenses for their products and offer them in very flexible scenarios, either directly or through partners.
 - machine-based licenses,
 - time-based licenses for subscription models and trials,
 - user-based licenses for roaming,
 - feature-based licenses — supporting a wide range of business models.
- SLP Online Service.
 - allows partners to do all of their license management without hosting their own servers.

More information on the Software License Protection Services approach for ISVs can be located at www.softwarepotential.com

These issues are tightly allied to the DRM/WGA/OGA approach being taken by Microsoft that is currently causing grief at many sites, and is likely to have far wider implications for managers and business using ANY kind of software.

**What SLP
Services
Do We
Need To Be Worried
About?**

Other Key elements extracted from the press release for Software Developers (ISVs) are;

- *"license and controls the application in whatever way the license states"* – given the way EULAs alter all the time this will be a nightmare to manage
- *"monitorable entities"* - this needs to be very clearly defined
- *"marketing now has a hook into license management"* – sales, more sales based on what they think we need
- *"easily turn on and off features"* – this needs to be very clearly defined, particularly where stealth data gathering might occur in the future
- *"gathering of monitoring data, (which can be used for things like billing, such as utility based billing at the end of the month)"* - data privacy principles need to be the governing principle here
- *"creation of statistics on what usage has happened within the application for future product planning"* – sounds reasonable but there has to be some definition and limits on what is gathered
- *"Creation of new digital licenses that will unlock and enforce features"* – this is a key issue about who has governance control over feature inclusions/exclusions at the desktop level.

Whilst application monitoring is an optional feature, the ISV needs to allow the end-user to opt in or opt out of a process without any penalty or reduced functionality.

**How Is
Microsoft's
Update
Services
Data Used?**

The data, your data, sent to Microsoft is used to operate and maintain the Update Services and is also used to generate aggregate statistics that are claimed to help Microsoft improve the availability and reliability of the Update Services.

To generate aggregate statistics, the Update Services use the GUID collected for several purposes:

- *To provide customers with the best possible service, the Update Services track and record the number of individual computers that use the Update Services and whether the download and installation of specific updates succeeded or failed.*
- *The Update Services record the GUID of the computer that attempted the download and installation, the ID of the item that was requested, whether updates were required, and configuration information about your computer (such as operating system version, browser version, and hardware ID).*
- *For versions of Windows prior to Windows Vista, the Update Services log an additional GUID if you provide responses about whether help and troubleshooting articles were useful in resolving your problem. This allows the Update Services to provide you with relevant information.*

**WGA
Notifications -
Download
and
Install
Telemetry**

Most of you are already aware (if not, now you are), that Microsoft is tracking your "system configuration " through Product Identification Data (PID) and Globally Unique Identifier (GUID) that is encrypted and reports back to their activation servers and verifies your eligibility to upgrades and downloads for software patches and fixes as well as add-ons and tools against a software manifest. Microsoft indicates that the PID & GUID contains encrypted hardware details, and no personal information to identify the individual.

The following information was extracted from Microsofts' UPDATE SERVICES Privacy Statement March 2007 at

<http://update.microsoft.com/windowsupdate/v6/privacy.aspx> which outlines the types of data collected and the conditions under which they gather data and statistics on your PCs.

Microsoft's Update Services collects information from your computer as follows;

- *What Microsoft software is on your computer, to help determine which updates are appropriate for your PC.*
- *The successes, failures, and errors you experience when accessing and using the Update Services (contained within a range of log files).*
- *Plug and Play ID numbers of hardware devices – codes assigned by the device manufacturer that identifies the device (e.g., a particular type of keyboard).*
- *Globally Unique Identifier (GUID) – a randomly generated number that does not contain any personal information. GUIDs are used to identify individual machines without identifying the user.*
- *BIOS name, revision number, and revision date – information about the set of essential software routines that test your hardware, start the operating system on your computer, and transfer data among hardware devices connected to your computer.*
- *Product ID – the unique product license identifier that is included with all Microsoft products.*
- *Product Key – the string of numbers and characters for Microsoft products, typically entered at installation/setup.*

When using the Windows Update or Microsoft Update web site they also collect information about the pages you visit. Windows Update is an opt in service except for steal the updates referred to at the start of this feature!

Update Services also collects some information about your computer ("standard computer information") that they claim is "generally" not personally identifiable. (For static IP addresses this may not be the case)

Standard computer information, as defined by Microsoft, is;

- your IP address, (if it is a dynamic IP address this may not be an issue, except when the data is in transmit mode)
- operating system version,
- browser version,
- your hardware ID (indicating device manufacturer, device name, and version), and
- your regional and language settings.

**Who
Do You Trust?**

Despite all the brouhaha over recent issues of stealth updates and WGA issues PCProfile would much rather trust Microsoft to verify, validate and offer updates etc, as long as we are made fully aware beforehand, of what they are extracting from our systems and that we are made aware of what files are to be updated on our systems and have the option of deferring, accepting or declining any updates.

However, when the same sort of approach is released under license through SLP Services to ISVs including small time software developers, a whole bunch of questions will be need to be asked by CIOs and IT Directors and answered by the ISVs to make sure systems are safe. eg;

- how will the ISV demonstrate they can be trusted to not snoop around systems, installing backdoors and root kits?
- what levels of systems control and server integrity over data will ISVs exercise?
- how will ISVs activate/track their own ISV licenses?
- what sort of uptime and service responses will the ISV provide when seeking assistance?
- what happens when the ISV becomes insolvent or goes out of business or is sold? How will activation then occur? Who will notify the end user customer?
- will the new vendor offer the same license conditions or will they turn on/turn off features and hold you to ransom for more money?
- will ISVs put their software source in escrow to protect larger organizations in the future?

**Just
When
You
Thought
All
Of
This
Was a
Beatup**

Malware has already been released posing as Windows Product Activation

In April 2007 malware identified by Symantec as '[Trojan.Kardphisher](#)' was downloaded onto systems to gather and collect credit card information from unsuspecting users who thought they were being asked to activate their software! See http://www.symantec.com/security_response/writeup.jsp?docid=2007-042705-0108-99 This trojan malware targets Windows XP users by portraying itself as related to Windows product activation.

<http://blogs.msdn.com/wga/archive/2007/05/11/malware-posing-as-windows-product-activation.aspx>

So, if they can do this using a Microsoft "look-alike" web page imagine what will happen when other vendor activation pages are cloned and presented in the same manner to phish for credit card and personal data.

The REAL RISKS!

Allowing any software vendor to access your PC without your knowledge and consent is fraught with danger. The ability of any software vendor to alter files without your consent, despite their altruistic intentions, leaves you vulnerable to attack vector approaches by trojans, spyware and other malicious code.

The ability of any software package to "turn on and off features" without your consent, in the name of statistical improvement or marketing is also a violation of your rights.

In our view, when Microsoft releases the Software License Protection Platform to 3rd party software vendors (independent software developers) then there could be real problems as the integrity of the code when released will be unable to be verified as being from a trusted source.

How will you know that the ISV hasn't included sleeper code within their application to harvest email addresses, and corporate data and then transmit this information to site/s where the data can be used against you in espionage, in trade secrets release or sale of intellectual property, or just plain marketing information gathering the names, addresses and contact details of all your suppliers and customers?

Should you be concerned? You should be, as this takes software management issues and risk mitigation to a much higher level, not previously contemplated.

If you are concerned, then you need to voice your concerns very loudly and clearly direct to Microsoft so that they can better understand the ramifications they are generating that could backlash against them.

VARIATIONS ON A THEME

If you think that the DRM activation issues that users face with Microsoft is enforcing with its own applications through WGA, OGA and DRM under Vista are a concern, wait until every other software vendor (ISVs) start coming up with varied combinations and derivatives on how they will "activate/control" your PC.

PCProfile's prediction based on experiences so far with existing activation issues is that when the source code is licensed via Software Licensing and Protection Services, it could progressively bring about massive disruptions to business systems as the ISVs come up with their own "innovative ways" to turn on/off software to control licensing usage!

The aim of the SLP Services is to benefit ISVs with innovative licensing strategies (and to curb piracy) and the benefits will need to be "sold" to the end user sites.

ISVs will be able to control software "features" using the SLP Services and will be able to "turn them on and off" based on whatever rule base they set in conjunction with the license to use the software.

It's not yet clear whether "activation in the manner Microsoft uses it" is embodied fully within the SLP services pack. No matter what form activation is listed within the source code for ISVs, the wider issues of activation techniques and server based activations will feature as issues to be wary of in future.

TO PONDER

Microsoft needs to be given, by CIOs and IT Directors, the very clear message (PCProfile is not saying jump to Open Source by making this statement) that the software once licensed correctly and installed, needs to be left stable and untouched until approved changes are allowed by the end -user, so that the business can operate without interference and without further activation/reactivation/validation. ie; activate once then go away and let the business operate under our control!

From PCProfiles' perspective letting the SLP source code out to ISVs is a huge risk that we all need to be very wary of and be as vocal as we can to make sure that system integrity and security is not destabilised in the name of improved piracy measures, and license controls!

Microsoft Software with Activation (September 2007)

Activation mechanisms now apply to the following Microsoft products;

The following items were extracted from <http://support.microsoft.com/kb/302806>

- Customer Service and Support Information
- Windows Vista Home Premium 64-bit Edition
- Windows Vista Home Basic 64-bit Edition
- Windows Vista Ultimate 64-bit Edition
- Windows Vista Business
- Windows Vista Business 64-bit Edition
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Starter
- Windows Vista Ultimate
- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows XP Professional
- Microsoft Windows XP Home Edition
- Microsoft Windows Small Business Server 2003 Premium Edition
- Microsoft Windows Small Business Server 2003 Standard Edition
- Microsoft Office Basic 2007
- Microsoft Office Home and Student 2007
- Microsoft Office Standard 2007
- Microsoft Office Professional 2007
- Microsoft Office Professional Plus 2007
- Microsoft Office Ultimate 2007
- Microsoft Office Word 2007
- Microsoft Office Visio Standard 2007
- Microsoft Office InfoPath 2007
- Microsoft Office Publisher 2007
- Microsoft Office Project Professional 2007
- Microsoft Office Project Standard 2007
- Microsoft Office PowerPoint 2007
- Microsoft Office Outlook 2007
- Microsoft Office OneNote 2007
- Microsoft Office Excel 2007
- Microsoft Office SharePoint Designer 2007
- Microsoft Office Student and Teacher Edition 2003
- Microsoft Office Professional Edition 2003
- Microsoft Office Access 2003
- Microsoft Office Excel 2003
- Microsoft Office FrontPage 2003
- Microsoft Office Outlook 2003
- Microsoft Office PowerPoint 2003
- Microsoft Office Publisher 2003
- Microsoft Office Small Business Edition 2003
- Microsoft Office Standard Edition 2003
- Microsoft Office Basic Edition 2003
- Microsoft Office XP Standard Edition
- Microsoft Office XP Service Pack 1
- Microsoft Office XP (Setup) Service Pack 2 (SP-2)
- Microsoft Office XP Application Error Report
- Microsoft Office XP Developer Edition
- Microsoft Office XP Document Imaging
- Microsoft Office Standard Edition 2003
- Microsoft Office XP Multilingual User Interface Pack
- Microsoft Office XP Pack for Tablet PC
- Microsoft Office XP Professional Edition
- Microsoft Office XP Service Pack 1
- Microsoft Office XP Professional Service Pack 2 (SP-2)
- Microsoft Office XP Proofing Tools Standard Edition
- Microsoft Office XP Small Business Edition
- Microsoft Office XP Service Pack 1
- Microsoft Office XP Small Business Service Pack 2 (SP-2)
- Microsoft Office XP Standard Edition
- Microsoft Office XP Service Pack 1
- Microsoft Office XP Standard Service Pack 2 (SP-2)
- Microsoft Office Web Components
- Microsoft Office XP Service Pack 1
- Microsoft Office XP Standard Edition for Students and Teachers
- Microsoft Access 2002 Standard Edition
- Microsoft Excel 2002 Standard Edition
- Microsoft FrontPage 2002 Standard Edition
- Microsoft Outlook 2002 Standard Edition
- Microsoft PowerPoint 2002 Standard Edition
- Microsoft Word 2002 Standard Edition

About the Author

PCProfile has been in the anti-piracy advice business for over 15 years offering assistance and advice to managers to help them save their own jobs and their businesses!

<http://www.pcprofile.com>

About "Managing Clouds and Moving Goalposts"

PC Profile has been providing anti-piracy (self-help / non-policing) advisory services worldwide since 1991 and is based in Adelaide, Sth Australia email:

pcprofile@internode.on.net web: <http://www.pcprofile.com>

PCProfile has been writing feature articles on a wide range of technology issues and many related to "management practices" or failing to understand what was happening around them. The key issues we noted were that technology changes were happening so fast around managers it was a bit like trying to "manage clouds". The other issue was the rules keep changing, (nothing new here) hence the reference to "moving the goalposts".

"Managing Clouds and Moving Goalposts" is a series of management focused articles on relevant technology issues that are impacting businesses across the world and are intended to inform with pragmatic solutions steps that can be undertaken to minimize risk.

Other articles in this series;

- Hasta La Vista www.pcprofile.com/Hasta_La_Vista.pdf
- Update Now - check the fine print before you click! www.pcprofile.com/Update_Now.pdf
- Is Your IP Leaking - 1 - Open Source www.pcprofile.com/Is_Your_IP_Leaking.pdf
- Is Your IP Leaking - 2 - Google Apps Risks www.pcprofile.com/Office_Collaboration.pdf
- RMA Your worst nightmare - www.pcprofile.com/RMA_Your_Worst_Nightmare.pdf
- Who Is Responsible for Software Piracy - 1 - www.pcprofile.com/who_is_responsible_for_software_piracy_1.htm
- Who Is Responsible for Software Piracy - 2 - www.pcprofile.com/who_is_responsible_for_software_piracy_2.htm
- The Risk of Old PCs www.pcprofile.com/The_Risk_Of_Old_PC.pdf
- We Dont Care How Much They Lose To Piracy www.pcprofile.com/We_Dont_Care_How_Much_They_Lose_Due_to_Piracy!.pdf
- Anton Pillar Raids - what they mean to your assets www.pcprofile.com/anton.htm
- No Budget for Software www.pcprofile.com/No_Budget_For_Audit_Software.htm

Microsoft, Windows, and all screenshots and weblinks are all recognized as both Copyright and Trademark terms of Microsoft Corporation, Redmond USA and are used in the context of this feature article as informational only.

Why "Managing Clouds?"

"As soon as you see them forming they change shape and form again, sometimes turning into vapour, other times dumping rain all over you!and you really can't manage them at all!"

The role of any manager is complex and difficult and with rapid changes taking place all around you it's difficult to know where to find practical advice on "how to manage" these changes. This is especially true when you think you have it all under control then find the rules change, again, and again.

This is when it's more like **"Moving the Goalposts"**!

USEFUL INFORMATION and WEB LINKS

For The Home User

To protect yourself against the sorts of Trojans that infiltrate your systems and other scams check out the information at <http://www.microsoft.com/protect>

Other Useful Information

To learn more about WGA Notifications see <http://www.microsoft.com/genuine/AboutNotifications.aspx>

For further information on WGA Notifications and Download and Install Telemetry see <http://blogs.msdn.com/wga/archive/2007/03/07/wga-notifications-and-download-and-install-telemetry.aspx> which shows an actual schema for the file data transmitted back to Microsoft.

<http://windowsvistablog.com/blogs/windowsvista/archive/2007/09/13/an-explanation-of-windows-update-automatic-updates.aspx>

Microsoft Update Blog <http://blogs.technet.com/mu/default.aspx>

How Windows Update Keeps Itself Up-to-Date
<http://blogs.technet.com/mu/archive/2007/09/13/how-windows-update-keeps-itself-up-to-date.aspx>

<http://www.itnews.com.au/News/61155,microsoft-updates-windows-without-user-permission-apologises.aspx>

http://www.informationweek.com/story/showArticle.jhtml?articleID=201806263&cid=RSSfeed_IWK_All

The behavior of reduced functionality mode in Windows Vista

<http://support.microsoft.com/kb/925582/en-us>

Error message when you start Windows Vista: "Your activation period has expired" <http://support.microsoft.com/default.aspx?scid=kb;EN-US;925616>

Addressing WGA validation issues

<http://windowsvistablog.com/blogs/windowsvista/archive/2007/08/25/addressing-wga-validation-issues.aspx>

Patents Apply

For those that have an interest in technical details, Microsoft has been granted patents for the processes used by Microsoft in validation and activation at the following links –

Method and system for licensing a software product MICROSOFT CORPORATION C/O MERCHANT & GOULD, L.L.C. P.O. BOX 2903 ... if not, then storing the PID, HWID and an identifier of a backend license in a database
... <http://www.freepatentsonline.com/20050216420.html> Microsoft Corporation.
Primary Class.: 713/200. International Classes: ... then storing the PID, HWID and an identifier of a backend license in a database;
<http://www.freepatentsonline.com/20020174356.html>.

Method and system for licensing a software product US Patent Issued on January 31, 2006 <http://www.patentstorm.us/patents/6993664-description.html>