

Migrating to Windows 7?

**What you need to
know about user settings.**

WHITEPAPER

TABLE OF CONTENT:

Executive summary.....3.

How Windows 7 compares to XP and Vista.....4.

The importance of user setting migration.....4.

User State Migration Tool (USMT).....5.

File or folder backups.....6.

How about Application Virtualization?.....6.

Security and migration6.

Enter User Workspace Management.6.

Summary.....7.

EXECUTIVE SUMMARY

On 22 October 2009 Microsoft plans to release Windows 7, almost three years after the general availability of its predecessor, Windows Vista. Windows 7 is expected to be the evolutionary upgrade to Windows Vista.

According an IDC research paper, around 50% of all business users will be using Windows 7 before the end of 2010.¹ In addition Gartner predicts that one-half of large organizations will skip Windows Vista and move directly from Windows XP to Windows 7.² For those on Windows XP, the predominant migration question is not "when" but "how". German automobile maker BMW, for example, has been running Windows XP in its broad client environment of 85,000 desktops since 2001. Happy with Windows XP, the automaker passed on Windows Vista, but is now planning for Windows 7.³

The general feeling at the roundtables is that the migration from Vista to Windows 7 should be a walk in the park, but the move from Windows XP may bring headaches to IT administrators for many moons to come.

This white paper discusses migration to Windows 7, specifically steps and elements you need to be aware of about end-user settings. Migrating to Windows 7 might seem straightforward; however, when it comes to end-user settings, there are a few items you need to carefully consider to allow for a successful migration without disrupting end-user productivity.

HOW WINDOWS 7 COMPARES TO XP AND VISTA

With Windows 7, Microsoft presents its latest iteration of their long-running desktop operating system (OS) line. If you passed on Windows Vista and are still running Windows XP, Windows 7 offers some important improvements over your old-and-counting OS. These include:

- 🔹 **Speed and performance**—Windows 7 beats XP in all performance benchmarks
- 🔹 **Compatibility**—While you may be able to continue to run XP for a while, you run the risk that future devices might not support the older OS
- 🔹 **Security**—Windows 7 provides much better “out of the box” security; it also doesn’t suffer from the annoying UAC prompts you see in Vista
- 🔹 **Design**—It goes without saying that a new OS will have a more contemporary design, but Windows 7 also offers a large range of customization, options, and features.

Furthermore, Windows 7 offers many new features plus some from Windows Vista that have been improved. Among these are:

- 🔹 **AppLocker** - Gives IT administrators the ability to control which applications are allowed to run on a user’s PC through the use of Group Policies.
- 🔹 **BitLocker and BitLocker to go** - Helps protect user data on their PCs as well as removable media by enabling encryption and backups of the recovery keys;
- 🔹 **DirectAccess** - provides seamless access to corporate networks without the need for a VPN connection.
- 🔹 **XP Mode** - A virtual guest operating system running XP in the background of Windows 7 for legacy applications that are not yet compatible with Windows 7.
- 🔹 **Problem Steps Recorder** - allows users to record the steps associated with a problem by capturing the screen shots and steps performed by the user and wraps up everything in a file that can be e-mailed to support. For most IT organizations the question will not be if they should migrate to Microsoft’s newest operating system but how to upgrade without disturbing the business operations.

THE IMPORTANCE OF USER SETTING MIGRATION

When it comes to operating system migrations, administrators know that this can be a very tedious and time-consuming task. Almost always, the end-users are affected in some way or another. It may be a simple setting within an application like the Microsoft Outlook signature or the layout and theme of the latest version of Microsoft Office. It could be more advanced user settings or files like desktop shortcuts, Microsoft Outlook nicknames file, or all the personal settings within the Microsoft Office suite of applications that are missing or no longer configured like they were before. Or possibly something more serious like user data that was never backed up or copied over to the new desktop during the migration or perhaps it was simply deleted as a part of the migration process. These things all contribute to users’ frustration and anger, lower user productivity, and business dollars lost.

Suppose a migration goes reasonably well and most users retain their information and data; how much time and preparation went into that project? Let’s take the following case, for example. Users leave work at close of business on Friday. In this organization the users are using a mixture of Windows XP and Windows Vista. On Monday when they return to work, they are now logging onto brand new Windows 7 desktops. This may be where the problems begin for IT and the helpdesk. Even though e-mails were sent out to let everyone know that the migration would take place this weekend, not all the users read or even saw that e-mail. IT administrators were very busy preparing for the migration so no training was given to the users on the new operating system. Users have no idea how to use the new system and are immediately confused and begin making calls to support such as: “Where is my data directory?” “Are all my documents safe?” “Where are things stored now?” “Where is the picture that was on my desktop last week?” These are questions that flood IT and the helpdesk whenever the user’s desktops or access methods change in the infrastructure. Unlike the technical staff of the organization, not all the users are aware that these types of changes are even taking place.

Over time, the desktop platform and the user’s experience has continued to evolve. Not just from a hardware perspective - moving from laptops and desktops to Terminal Services and remote applications - but also in terms of the multitude of operating systems hosting their experience. Users have begun to make the computer and their sessions more and more personal. Personal settings or “Personality” can range

from such items as background pictures, customization of the applications, e-mail signatures, and frequently-viewed Websites stored in their browsers. They might even include alterations to desktop background color, the location where their data is stored, or the printers they have access to. No matter what the situation is, all these things contribute to the user experience and make up the user's Workspace. IT has begun to realize that the user's workspace has become important to the user's overall satisfaction in the workplace and to simply disregard these settings can no longer be an option for administrators. Now, the problem that IT is faced with is how to retain all these settings during migration to a new Windows platform and maintain the ability to deliver a persistent Workspace to the users before, during and after the migration process, without interrupting business operations. Many organizations lean on a vast amount of tools and utilities to help ease their mind during the desktop migration process. These tools and utilities include the likes of policies, scripting, folder redirection, cloning, imaging, application streaming, computer virtualization, file copying, backup and restores, user migration tools, etc. These are all good tools and utilities but they do include some complexities and administration overhead to use them and they are also time-consuming to implement or maintain long term.

USER STATE MIGRATION TOOL (USMT)

Windows 7 ships with a new version of an old tool called the User State Migration Tool (USMT). USMT is a part of the Windows Automated Installation Kit. It provides an elegant way to migrate user settings and files from the old Windows XP system to Windows 7. The upside to USMT is that it performs the migration during the installation of the new Windows 7 OS and retains all the proper permissions maintains all the proper folder layouts and locations. Since the USMT keeps all the data local to the machine (it stores the data in a Windows.Old directory), it takes minutes rather than the hours that a backup to a USB drive or a file share would consume. But, with the good comes the bad. It is a manual process and does require some pre-configuration. The process has to be done on each machine that is to be upgraded and the user responsible for the migration needs elevated privileges to perform the operation.

GPOs and scripts

Prior to desktop migrations, most organizations have already put in place the steps to try and smooth the transition from the existing desktop OS to a newer one. A well-established Active Directory structure is usually up and running and user

and computer accounts are generally organized according to the design of the company. E.g. Organizational Units (OU) in some cases represent the geography or the business units of the organization. Each OU is broken down further into smaller branches or sub-divisions which include PC and user accounts. Each of the OUs can have one, or possibly many, Active Directory Group Policies Objects (GPOs) and/or logon scripts attached to them. These GPOs are used to control user behavior, allow access to resources, map drives and printers, or copy data to or from the user's session to another location on the network. The more advanced scripts and GPOs redirect user information and data from the user's profile to a central location on the network in order to attempt to capture user "personality" for a desktop operating system migration or in the event of a disaster.

These methods seem to provide good solutions and in some cases may alleviate a good percentage of the risk, but policies and scripts do not scale well, neither do they capture all of the user's personal settings. Furthermore, if we look beyond the one physical desktop each user is assigned to, and look towards the possibility of multiple types of access across multiple operating systems, both physical and virtual, those GPOs and scripts may no longer be applicable to all of these scenarios. For example, administrators may be redirecting the My Documents folder on the current XP desktop to a central location or the user's home directory. What if the physical machine is upgraded to Windows 7? Has the data been saved? Will the settings migrate easily to the new OS? Will the current scripts and GPOs still be relevant to Windows 7 or will they need to be reworked? Is the folder location the same?

This is just one example of user settings but there are many others to consider. User personality is made up of several settings that are not held in the traditional redirected folders that GPOs have access to. Some settings are held in the user registry or the profile, nested way down in hidden folders that are not accessible with GPOs and are too complex to handle with scripts.

FILE OR FOLDER BACKUPS

File or folder backups are taken pre-migration and used to save user personality and restore settings to the new desktop platform. This is usually done by way of file shares, USB drives, tape drives, the use of utilities like batch file scripting or file copy commands. This is a mainly manual and very tedious process; it does not always lead to a proper transition and is prone to human error. One thing to consider when performing a backup or a file copy is that permissions might not be retained or properly transfer to the destination folder or file system nor are the application settings carried over. Secondly, the folder structure on the new OS might not be the same so data and settings may not be placed in the proper location. Improper or incomplete file copies leave users without access to data or their personal settings from the previous OS.

Some organizations claim to have control of the desktops prior to a migration and they control all of the applications that are installed on the desktops through manual installations, Group Policies, or some types of application automation software. The real trick is whether or not those applications are compatible on the new operating system. From this standpoint, application trending, reporting and an inventory of the locally installed applications become critical to the success of the migration. Users will need the same applications tomorrow that they had yesterday.

HOW ABOUT APPLICATION VIRTUALIZATION?

Is application virtualization is the answer? Well ... sort of. Application virtualization does indeed solve some of the compatibility issues previously mentioned as virtualizing the applications decouples the applications from each type of OS. But what about the user settings that accompany each application? These settings are still held in the user's local profile and still need to be persistent on the hosting operating system for the virtual application to work as expected. As the name implies, a local profile is a user profile that exists on a single machine. Local profiles lead to end-user confusion as applications and environment changes do not follow the users when they log on to different desktops or roam between physical and virtual machines. For example, a user may change their background setting to green on one device, log out, and then log back on to a different device to find that the background is not green. This is caused by having two separate local profiles, one on each machine. The settings do not move with the user and therefore they will not move to the new operating system post migration.

SECURITY AND MIGRATION

The last factor to consider on the subject of a desktop migration is the security around the desktop both before and after the migration. Some companies take the opportunity to re-evaluate whether or not the desktops are locked down enough to minimize the management of the workstation. Gartner placed users in four types of management categories: base, somewhat managed, moderately managed, and well managed. These categories are defined as follows :

- Base - This is a wide-open scenario. Users can install applications and change settings, with few to no management tools used.
- Somewhat managed - Users are limited to a narrow list of tools and utilities for patching or performing an inventory of the system. Users are administrators on their own machines.
- Moderately Managed - Users have access to tools and utilities for patch management but policies are not implemented. Users are usually administrators on the machine.
- Well Managed - Users are no longer administrators on their machines and policies and procedures are in place.

By removing the administrator role from the users, administrators can start controlling the infrastructure and how services are delivered, while maintaining security and limiting unauthorized changes to the machines. In doing this, they lower their total cost of ownership (TCO), reduce the management complexity and the machines are more secure and reliable.

ENTER USER WORKSPACE MANAGEMENT.

With all this in mind, what is the best approach to take best order to guarantee the success of a full migration to a new operating system? Pause for a moment to recap what has been discussed in the last few pages... A User Workspace is made up of a number of unique elements including browser settings, desktop settings, application settings, printer settings, personal data, environment variables, personal e-mail profiles and essentially any individually customizable element that enables them to accomplish their assigned job. But it also encompasses the user's context such as time of day, location, device type and even the user themselves.

IT organizations should consider the use of solutions that enable the awareness of user context and personality for their users. These types of solution go above and beyond the limitations of native Windows user profiles and central administration tools such as Group Policy. They enable

users to experience a common and familiar workspace no matter how the workspace is delivered and regardless of the underlying OS. This gives IT administrators the power and control to automatically provide the right applications, the right printers and the right data to users based on who the user is as well as where, when and how the user is connecting. A user workspace management product decouples the user's customizations from the underlying operating system. Individual customizations are stored on the network and transferred to the local device as the user begins work with it. When users make additional customizations, those changes

are replicated to the external location through an automated mechanism. Thus, the only steps necessary to ensure that user data is retained during a refresh is to simply log a user off and log the user back on. This single step can automatically transfer personality information down to the user's refreshed computer, allowing the user to immediately return to work. Administrators need a user workspace management product, as well as the skills and the time to redesign their user settings management so it can be suitable for multiple application delivery methods across various operating systems.

SUMMARY

The upgrade from Windows XP to Windows 7 is unique. In this particular upgrade, profiles between these two operating systems are completely incompatible. Thus, any upgrade from Windows XP to Windows 7 can require an extensive and painful manual migration of settings from the old instance to the new one.

Organizations that leverage the use of a user workspace management platform gain the required automation for OS upgrades, including migration to Windows 7. Personalization elements are decoupled from the OS within such a platform, so the process to reapply those settings to a new OS version becomes inconsequential.

Along with RES PowerFuse 2008, RES Software supplies User Workspace Management software. Whether the desktop is VDI or server-based, Windows XP or Windows 7, streamed or traditionally managed, and whether streamed, published or standard applications are being used, RES PowerFuse gives users their own personalized desktop where and when they need it, with their own personalized settings always available. RES PowerFuse makes it easy to personalize the workspace to create a tailor-made experience for the user for the duration of the user's session. This increases end-user productivity and satisfaction even through a major infrastructure change like a desktop migration.

- 1) Worldwide Windows Client Operating Environment 2009-2013 Forecast: Windows Vista to Give Way to Windows 7, IDC, May 05, 2009
- 2) Getting Off Windows XP Is More Important Than Windows Vista vs. Windows 7, Michael A. Silver and Stephen Kleynhans, Gartner, March 12, 2009
- 3) BMW and Windows 7: Three Reasons Why the Car Giant Is Upgrading Now, Shane O'Neill, CIO, September 03, 2009
- 4) Toolkit Best Practice: TCO Comparison of Desktops vs. Notebooks, 2008 Update, Federica Troni, Gartner, March 18, 2008

RES Software is the leading provider of User Workspace Management software. Since 1999 we have enabled our more than 2,500 customers worldwide to compose and manage personalized and secure workspaces for their end users. Our Workspace Management products bridge the gap between traditional desktop management, thin clients, and virtual desktops. The business benefits our customers have realized by using our products include a lower TCO, broader security and an increased productivity. RES Software is a global company with nine offices across Europe and the U.S. RES Software products are exclusively delivered through a network of certified partners.

More information: www.ressoftware.com

