

November - 2010

***Windows 7 Upgrade Risk Mitigation Planning:***  
*Ensuring Windows 7 Upgrade Success*

**By:**

*Robert Schaper, Laplink Software Enterprise Solutions*

## Contents

<b>Introduction</b>	<b>2</b>
<b>Risk and Cost</b>	<b>2</b>
<b>Upgrade Strategies</b>	<b>3</b>
<b>Creating a Risk Mitigation Plan</b>	<b>4</b>
<b>Implementation</b>	<b>6</b>
<b>Summary</b>	<b>8</b>

### **Abstract:**

Organizations upgrading to Windows 7 are assessing strategies and tactics for introducing the latest desktop OS from Microsoft to their end-users, and some early adopters are citing un-forecasted costs and business impacts with the overall effort. This white paper outlines the summary feedback from early adopter organizations and covers what has been done to minimize risk, lower costs, and shape the new Windows 7 user experience from the onset with PCmover Enterprise.

This white paper is intended for anyone involved in strategic planning and policy making for Windows 7 upgrade projects. Whether the migration is a "fork-lift" upgrade project for all PCs in an organization, or using a "replace as you go" method only for machines refreshed, the process represents both risk and opportunity to businesses.

## **Introduction**

Organizations in the process of finalizing Windows 7 upgrade and PC refresh initiatives can optimize their strategy and significantly reduce risk and hidden costs by leveraging best practices and concepts outlined in this White Paper.

Avoiding the policy creation and planning stages can lead organizations to a very costly experience when choosing to upgrade, as end-users will not be able to work properly, helpdesk support staff will be overtaxed, third-party service fees will grow, and the amount of lost data will be significant.

With careful planning and a sound migration policy framework, the Windows 7 upgrade process can be a seamless, scalable experience across the entire project.

## **Windows 7 Upgrades – Risk and Cost**

According to recent analyst research (Gartner & IDC, Aug/Sep 2010) , business impacts from Windows 7 upgrades within unmanaged and mixed-managed IT environments can exceed \$1,200-\$3,000 or more per PC upgraded, quickly straining resources, budgets, productivity, and end-user morale throughout the migration effort.

In addition, many organizations simply do not have the staff or resources to execute on a full organizational upgrade in a predefined time period. Instead, these organizations are choosing to introduce Windows 7 only at the "end of life" of the previous machine, or upon a fixed lease refresh schedule.

The cost in upgrading a user in this manner has much deeper business impacts than planned migrations, as the end-user downtime, data-loss, software media loss, and overall impacts to the business are significant.

## **“Fork Lift” vs. “Refresh” Upgrade Methodology**

As business stakeholders approve the Windows 7 upgrade initiative, they will also likely approve the method of introducing Windows 7 into the business. This is called the Migration Policy Statement.

As a fundamental choice, the migration can be introduced to everyone that qualifies in a specific time-period (weeks or months). Alternatively, organizations on a fixed refresh schedule or wishing to keep short-term costs low may elect to introduce Windows 7 to end-users receiving a new machine only.

The costs of maintaining a dual Windows XP and Windows 7 desktop OS environment can be more significant long-term, so the decision to move quickly or slowly comes with a cost-benefit requiring careful analysis.

After completing the Windows 7 upgrade Risk Mitigation Plan, the re-adjusted cost to upgrade each PC may justify a “fork lift” upgrade approach accelerating Windows 7 adoption and anticipated benefits.

## **Unique Migration Technology**

Laplink Software is the pioneer in PC transfer, and has continued to innovate solutions to automate the Windows 7 upgrade experience. Laplink’s core enterprise migration solution, PCmover Enterprise, is the only migration solution capable of migrating installed applications, user accounts, settings, and data *independent* of hardware or Windows OS. This allows IT organizations to overcome issues and challenges with upgrade processes that impact the end-user, cause data loss, and increase the overall cost.

PCmover Enterprise is also the only migration solution that places policy management capabilities in the hands of the non-technical user. Whether the level of automation or filtering needs to be changed for one user, group, or role to another, PCmover Enterprise eliminates the need to edit XML, retest, and re-deploy with each change.

Since business stakeholders assume an extended time to complete a fork-lift upgrade when initially evaluating, the short-term cost can be re-evaluated with PCmover and a lower cost, reduced risk strategy can move forward.

## **Seeking Rewards from Optimization**

Optimizing the desktop upgrade strategy by using PCmover Enterprise within a carefully planned Risk Mitigation Strategy will have immediate and long-term benefits:

### **Benefit 1 – Reduced Risk**

**Finish Sooner.** Windows 7 upgrade and PC refresh projects are finished in a shorter timeframe, requiring fewer resources to complete.

## Benefit 2 – End-User Satisfaction

**Reduce IT Resource Needs.** Post-migration support issues and end-user downtime is minimized, establishing a higher end-user satisfaction baseline.

## Benefit 3 – Return on Investment

### **Return on Investment.**

Organizations that choose to optimize their upgrade path with PCmover Enterprise stand to save \$300 *or more* with every PC upgraded or refreshed.

## **Creating a Risk Mitigation Plan**

Promoting a sound risk mitigation plan associated with a Windows 7 upgrade initiative to business stakeholders will help generate risk-reward thinking needed to make a decision and move forward.

Once the risk mitigation planning is completed and business owners, key stakeholders, and power users have aligned on project objectives, the Windows 7 adoption strategy will look more like a comprehensive, holistic business initiative than an IT upgrade project.

Without a well thought out risk mitigation plan and a coordinated business mission statement supporting the Windows 7 upgrade initiative, businesses and IT departments will find frustration, unnecessary costs, and extended

timelines for supporting dual OS environments.

Contents of a developed risk mitigation plan will include these elements:

**1. Mission Statement.** A clear set of measurable and achievable objectives, typically defined within a “mission statement” incorporating the needs of the end-user community and expected business impacts, will be essential.

### **2. Application Compatibility Policy.**

Application compatibility is a major barrier to upgrading users to Windows 7, but with careful planning can be easily managed.

### **3. Deployment and Migration Policy.**

Designing a set of guidelines for deploying images and migrating user data, applications, settings, and user accounts is critical to avoiding delays and minimizing unforeseen issues. This could include determining 32-bit vs 64-bit OS policies for users, for example.

**4. Cost and Resource Analysis.** Before moving forward with a Windows 7 upgrade initiative, IT organizations must work to identify cost centers, both hard and soft, as well as develop strategies to reduce short and long-term impacts.

**5. Pilot Project.** Before jumping in, start with a sub-set of capable users responsible for providing thoughtful feedback on the initial experience and identify ways to improve before deploying more broadly. The pilot project will also help identify the phased roll-out strategy most suitable for each user group or scenario.

## 6. End-User Post-Migration

**Analysis.** Collecting ongoing feedback about the Windows 7 upgrade process and refreshing application compatibility policy, migration policy, and cost analysis factors will establish long-term improvement practices. This can be done with end-user post-migration interviews, and/or surveys.

### Solving for Application Compatibility

IT service professionals with Windows 7 upgrade project experience likely already know that application compatibility is a major barrier to moving forward with an upgrade if not properly controlled for. With proper planning and solution design, risks associated with application compatibility can be minimized and Windows 7 project success can be effectively realized.

You can manage application compatibility proactively by keeping an accurate list of all programs in use in your organization, creating an “application portfolio.”

#### Application Compatibility Steps:

- Create an application inventory
- Identify problems and prioritize solutions
- Develop Black-List
- Identify software packaging needs
- Remediation Plan vs Virtualization

Careful analysis and planning will contribute to risk reduction regarding application compatibility, and streamline the upgrade experience for users with custom in-house developed applications, as well as other line-of-business programs.

### Creating an Application Inventory

Managed environments present less hurdles to the inventory process because applications are packaged, and installations are controlled or prevented (unless approval is granted to the end-user). A managed environment will most likely already have a list of supported and approved applications, and you can view this list as complete for all managed computers.

An unmanaged environment is challenging due to the complex task of discovering all the applications installed, both officially supported and approved applications, and the programs that users have installed on their own.

Most organizations fall somewhere in the middle of this range: they have a combination of a central repository of applications and images, and a number of applications that are exceptions to the standard throughout the organization. In addition, decentralized IT infrastructures have a more complex task of communicating their individual inventories across organizational, cost center, and geographical boundaries, presenting an additional set of challenges during the planning stages.

### Available Inventory Tools

Organizations using software management tools such as Microsoft Asset Inventory Service (a tool available through Microsoft® Desktop Optimization Pack for Software Assurance), Microsoft System Center Configuration Manager 2007 (SCCM), or Microsoft Systems Management Server 2003 (SMS) may already have a comprehensive list of applications present in the organization.

Organizations without centralized management software will need to select a tool to gather application inventories. Although it is possible to take an inventory manually, you will run the risk of making mistakes and omissions. An inventory tool can effectively gather the list of applications running on every computer. The Microsoft Application Compatibility Toolkit 5.5 includes an inventory tool automating the process for decentralized organizations.

### **Application Inventory – Streamlining**

The number of machines will factor when capturing the application inventory, so reducing the number of computers to be inventoried if they are managed (users cannot install their own software) and identifiable is important. Determining a sub-set of computers from each specific role and location to gather an inventory is one method. In lightly managed or unmanaged environments, users may be permitted to install their own software, pushing the number

of non-standard applications installed into the thousands, even for companies with only 250 employees.

The number of user roles will also affect the total scope of the inventory, since including representative computers from each role to ensure proper coverage is necessary to get all roles covered.

### **Creating Inventory Manually**

Highly decentralized and unmanaged organizations may opt to manually collect application compatibility data. The manual process can be done by creating a spreadsheet listing the applications on each computer, gathered from the Start menu and add/remove programs. The accuracy of this method will be impacted by applications installed on a per-user basis (not visible after logging in), and by the accuracy of the manually collected data.

The manual application inventory process is not recommended for mid-market and enterprise upgrade projects.

### **End-User Interviews – Large Enterprises**

Larger organizations would expand these techniques to include interviewing representatives from each department to help the application compatibility team create a list of applications used by that department. These interviews can also work to protect third-party service providers involved in the migration process, presenting an opportunity to clearly communicate what is expected in the migration and upgrade process.

### **Analyzing Application Compatibility Data**



Before moving from the inventory phase into actual testing of applications, hard decisions will need to be made regarding application priority and the applications and versions to be officially supported after the deployment is complete.

*Application redundancy:*

Your organization has more than one application performing the same tasks.

*Application relevancy:*

Your organization has multiple versions of an application including outdated and unsupported versions. Depending on the application and your infrastructure, you may want to check on application-to-application dependencies before moving to an entirely new version of a particular application.

*Application necessity:*

Your organization has applications that are irrelevant to the day-to-day work being done in your organization.

You can use the application inventory to reduce application redundancy. For example, your organization might have multiple applications used to create graphics. By selecting a single application, and a single version of that application as a standard, your organization can save money spent on support. If you identify a version of your required application that is proven compatible with the version of Windows operating system you are

deploying, you can also reduce deployment testing by focusing on this single application and version.

The next step is to categorize the applications into groups based on the relative importance of that application within your organization. To understand this, you will need to work with the business owners of each application. Some applications are considered business critical, such that your business will halt if the application fails or is unavailable. Other applications are very important, but there are ways to keep some business going if they fail. Although the individual terminology may vary, here are some common priority levels to consider:

*Business Critical:*

Applications that stop your organization completely if it fails should be considered “business critical”. If in doubt as to whether an application falls into this category, consider whether the organization can make any money while the application is unavailable, and whether personnel can continue working at all without the application. If this application fails in the middle of the night, how long it would be until your pager goes off?

*High Priority:*

Applications performing a vital role in a department or across an organization are considered “high priority”. A failure in a high priority application may disable a department or a single business function in the organization. If a high priority application fails, the organization can continue doing business, but one or more departments may be seriously hindered.

*Important:*

An important application that is used frequently, but will not cause a stoppage of work if it fails is considered “important”. An example would be a spreadsheet or word processor application that is widely used, but not related to a fundamental business function.

*Optional:*

Approved applications limited use and not directly related to a business function are considered “optional”.

Assigning priority levels to applications is often a subjective process, and may be subject to periodic revision. One way to supplement the priority analysis includes the review of SLA agreements for specific applications. If the SLA requires addressing the issue in a matter of minutes, it should be considered for “business critical”. If there is no SLA agreement, then it might be considered only “important” or “optional”.

## Identifying Applications for Specific Roles

The concept of user roles can be helpful in determining the components of specific operating system images for deployment. By separating your user base into specific roles, you can more easily define the applications to be layered on top of the operating system image. For example, if you define a user role of accounting, you can specify that, in addition to the

operating system, the users in this role will receive Microsoft® Office and the organization’s standard accounting software.

Some possible roles might include:

- Human resources
- Information worker
- IT support desk
- Marketing
- Developer
- Executive

Role based analysis may not be an efficient way to capture all users, especially for larger organizations that have much larger breadth and depth in the types of roles across the business.

## Establishing a Migration Policy

To create an optimized migration experience in the enterprise, a unique Windows 7 upgrade utility like Laplink PCmover Enterprise offers non-technical users with a quick way to deploy and manage migration policy. The traditional way of deploying new PCs and upgrading users with scripting and manual methods of migration has proven very costly for early adopters, driving many IT organizations to evaluate third-party utilities and services to support the upgrade.

PCmover Enterprise includes an enterprise-class Policy Manager and a no-install migration utility for easy deployment across networks, as well as, remote users. Instead of having to design and implement a fully custom script supported by a scripting expert, limiting the entire enterprise to one defined process, PCmover Enterprise instead puts the migration process in the



hands of the IT analyst or business stakeholder.

Policy Management Options Supported\*\*\*:

- Domain and Local User Accounts
- Black Lists
  - Applications
  - Data: File types and Folders
  - User Accounts
- Reporting
- Automation
- Connectivity Methods
  - Laplink USB
  - Network
  - File-Based
- Upgrade Methods
  - Old to New machine
  - In-Place
  - VHD Recovery

\*\*\*Note: For full details on PCmover Enterprise policy support, please request the "PCmover Policies" document from a Laplink Corporate Account Executive ([corpsales@laplink.com](mailto:corpsales@laplink.com)).

## Conclusion

Many organizations evaluating the migration to Windows 7 quickly realize the entire desktop infrastructure will be affected in some way, and thus evaluate ways to minimize the short-term impact. Including limits on Windows 7 adoptions. In order to reduce the risk and cost associated with the upgrade short-term and reduce the timeframe for managing dual-OS environments, Laplink has worked to design an automated method for enterprise IT service teams and

personnel to implement without the involvement of advanced technical users.

**The result: Your organization will have a recipe for upgrading to Windows 7 in less time, and with a lower overall total cost to upgrade.**