

ALTIRIS.  
SMART MOVE.



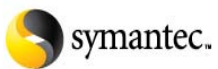
## Create a More Manageable PC Fleet with Vista Migration

ALTIRIS: NOW PART OF SYMANTEC



# Table of Contents

Introduction .....	1
Vista Migration and Implications for Asset Management .....	1
Migration Best Practices: The Altiris Six-Step Process .....	2
Step 1: Pre-Migration Readiness Assessment.....	2
Step 2: Data and Setting Preservation .....	2
Step 3: Image Build Process .....	2
Step 4: Application Packaging and Compatibility .....	3
Step 5: Migration and Configuration.....	3
Step 6: Post-Migration Reporting .....	3
Realizing Continued Benefits After Migration.....	4
Infrastructure Management Costs .....	4
Automated Asset Management .....	5
Maximizing Long Term Benefits with Intel vPro Processor Technology ...	6
Summary.....	7



## Introduction

Migrating to Microsoft Vista offers more than the latest in operating system (OS) technology—it is an opportunity to improve the way devices are managed and to reduce long-term maintenance costs. The fundamental mission of IT groups is to support existing infrastructure and applications while executing new initiatives. For IT staff, the first imperative is to ensure mission-critical systems continue to function without disruption to business operations. At the same time, businesses depend on IT to deliver innovative solutions that allow the organization to adapt to changing market conditions. An obvious question arises: How can IT executives maintain a growing set of applications and introduce new initiatives with relatively fixed resources?

One solution is to optimize the maintenance process and free resources for new initiatives. Consider how widely the allocation of IT resources can vary. According to Forrester Research, a typical company will allocate 25% of its IT budget to new initiatives, with 75% required for ongoing operations and maintenance. A company receiving poor value for its IT investment will spend only 15% on new initiatives; exemplary companies will require 60% of their IT budget for operations and maintenance, leaving 40% for new initiatives. (Source: “APM Tools Will Reach \$500M To \$700M By 2008, Phil Murphy,” Forrester, 7/22/05) Clearly, initiatives that improve operations benefit new initiatives as well.

Vista migrations that employ Altiris' automated Client Management Suite coupled with improved device control from Intel® vPro™ processor technology establish the foundation for more efficient long-term device management. Leveraging the opportunities presented by a Vista migration to introduce best practices in asset management will yield benefits long after the upgrades are completed.

## Vista Migration and Implications for Asset Management

Microsoft Vista offers many improvements over its predecessors, ranging from better searching and an enhanced interface to superior security and manageability—there is a cost, though. Vista demands more resources than is available on a significant portion of deployed client devices. This is not uncommon with major OS upgrades, and like past migrations, many analysts predict the OS migration will coincide with a hardware refresh. Clearly, the question is not whether to upgrade to Vista but when.

Another question that is just as important but tends to garner much less attention is how to upgrade. There are a few basic options:

- Migrate all clients at once—This method is highly manageable but expensive.
- Create a minimal number of different configurations and migrate these groups in batches—This option balances cost and manageability but may not fit with other organizational constraints, such as migrating entire departments at once.
- Gradual migration coordinated with hardware refreshes—New hardware is purchased and once a large enough set of new PCs are in place, the entire set is migrated to Vista. For example, an entire department may migrate to Vista at one time.

Many who have participated in enterprise migrations in the past can tell stories of best-laid plans gone wrong. Migrating all clients at once can wreak havoc for days or longer when the inevitable exceptions and errors occur. PCs thought to have one hardware configuration have another—either accurate inventory records were never kept or they were not up to date. To minimize the chance of delays and disruption, OS migrations should follow a formal procedure that accounts for the likely issues that will arise.

By automating the key processes involved in a migration, including personality capture, imaging, application deployment, and personality restoration, Altiris significantly reduces the amount of time spent by the IT function. Industry estimates indicate a reduction of 75% in IT efforts using automated tools such as the Altiris' Migration Suite. For an organization with 1,000 PCs, that results in a savings of 2,920 person-hours (Source: Microsoft Window Vista Migration: Addressing the issues of operating system upgrades and migration, Butler Group October 2006). In addition, the best practices lay the foundation for the automation of long-term management of IT infrastructure and further cost reductions well into the future.

## Migration Best Practices: The Altiris Six-Step Process

The Altiris Six-Step Process encompasses essential elements of a successful migration: understanding the starting point of the current infrastructure, preparing for the migration, and finally, executing the migration. These high-level elements are broken into six steps.

### **STEP 1: PRE-MIGRATION READINESS ASSESSMENT**

In the initial stage of the Altiris Six-Step Process, the goal is to clearly understand the hardware, software, and deployment resources required to complete a migration. This step includes:

- Completing an asset inventory
- Determining whether hardware meets upgrade requirements
- Determining software licensing implications of a migration
- Determining security implications of a migration (and areas that can be improved via the migration)
- Assessing the network infrastructure to put plans in place for migrating remote offices that may have lower bandwidth available.

At the end of the first step, one will understand the scope of the migration, know of any hardware deficiencies, and understand constraints on the process, particularly with regards to remote sites.

### **STEP 2: DATA AND SETTING PRESERVATION**

Migrations have to preserve data and, as much as possible, maintain user-defined settings. Imagine even a moderate-sized migration in which users lose printer configurations, drive mappings, and other OS configurations. This failure of one part of the migration can alone create significant demands on the service desk and cost hours in lost productivity for each user.

To ensure user-defined configurations are maintained across the migration, you must create profiles that capture the "personality" of each device, including network drive mappings, printer mappings, desktop configurations, application templates, and system settings as well as user documents. Migration managers must be careful to capture configuration settings for custom applications as well as popular desktop software.

### **STEP 3: IMAGE BUILD PROCESS**

In some cases, very large enterprises with tens of thousands of clients have migrated with a single image, but others may need a number of different images. With the proper tools, systems administrators will be able to create a small set of base images that can be further customized by deploying additional applications during migration and configuration. The ideal scenario is to build an image on a freshly formatted drive with only the OS, service packs, security patches, and baseline configurations. Some vendors recommend that all organizations should strive to have just one, single, hardware-independent image for all of their hardware. Although this is achievable using the Altiris toolset, we recommend that customers carefully consider the costs versus benefits of a single image (which can be very costly and time-consuming to assemble) versus maintaining a small set of images.

#### STEP 4: APPLICATION PACKAGING AND COMPATIBILITY

To maximize flexibility, applications are not included in the baseline image. Instead, they are installed after the OS using automated processes that deploy only applications needed based on roles and functions of each user and their PC. With automated software delivery, applications can be prioritized and rolled out incrementally.

#### STEP 5: MIGRATION AND CONFIGURATION

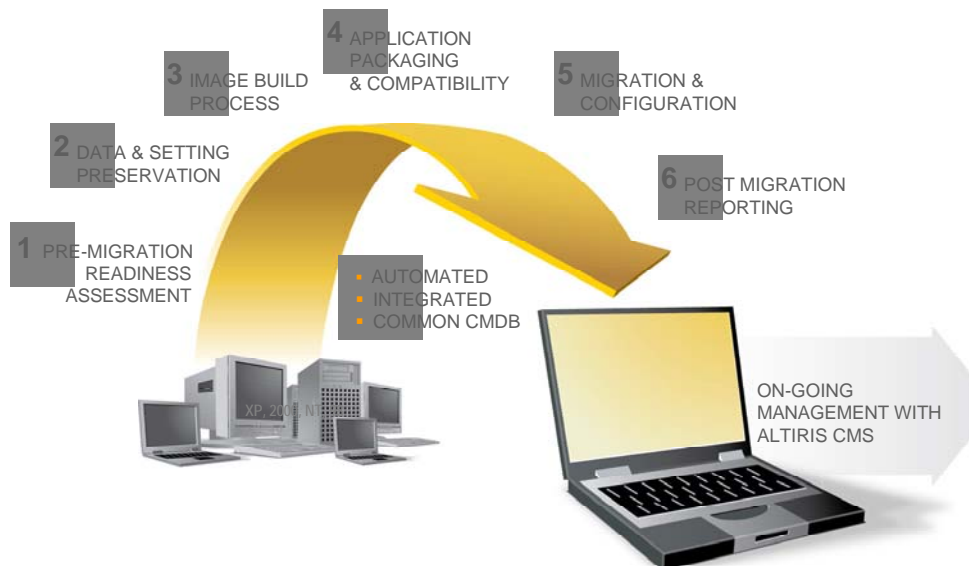
At this step, planning is complete and the migration is executed. The core migration components, the base images with the OS and application packages, are deployed to PCs. Once the core components and the applications are successfully installed, the next step is to restore the computer's "personality." The profile that was created in Step 2 is now used to reconfigure the PC to the same (or at least similar) customized state that existed prior to the migration.

#### STEP 6: POST-MIGRATION REPORTING

In the last step, metrics are generated to assess the success of the migration, including:

- The number of devices successfully migrated
- The number of applications deployed
- The number of user configurations successfully migrated
- The number of clients with operations pending
- The number and type of problems encountered during imaging and application deployment

The goal of this step is to provide administrators and managers with a clear picture of the state of the migration and a baseline for future asset management.



**Figure 1: The Altiris 6-Step Process addresses the key steps in OS migration and lays the foundation for efficient long-term asset management.**

## Realizing Continued Benefits After Migration

The end of a migration is the beginning of another phase of asset management. On any given day, an IT administrator may be rolling out new hardware, installing new applications, patching client devices, and redeploying servers in addition to other common asset management tasks. Essential elements of asset management include:

- Deploying devices and applications
- Ensuring quality of service (QoS) levels are maintained
- Maintaining a service desk and responding to incidents
- Patching devices and managing configurations
- Redeploying resources according to changing business needs
- Monitoring operations and ensuring continuous compliance

It is useful to think of these tasks within an asset management life cycle. The process begins with the deployment, moves through maintenance and redeployment phases, and concludes with device or application retirement.



Keeping track of fine-grained details in a large infrastructure is virtually impossible without automated tools; trying to operate without tracking those details ultimately drives up the cost of ownership.

### INFRASTRUCTURE MANAGEMENT COSTS

In addition to framing management operations, the infrastructure life cycle is useful for understanding the total cost of ownership (TCO). Although the initial cost of acquiring assets is clear, and the licensing and support contracts are annual reminders of some of the ongoing costs, there are many smaller, sometimes forgotten costs that—multiplied over hundreds and thousands of clients—can quickly increase the TCO.

Consider a typical problem with the increasing popularity of Web-based applications. As we move to rich Internet applications, developers make greater use of Java and .Net technologies. These applications depend on a particular client configuration, such as a browser supporting Java version 1.5. Now imagine a user running a Web-based application that fails to execute an operation correctly. The user contacts the service desk; a support technician spends several minutes diagnosing the problem over the phone and then goes to the user's desk to install the proper components. The cost of lost productivity and the ongoing costs of maintaining a service desk that can respond to these problems could have been much lower.

Another version of this scenario could start with the same problem but change once the service desk is contacted. If the service desk technician has access to a configuration management database, the technician can quickly determine the incompatibility between the client device and the application. Next, using software deployment tools, she can push the correct version to the client and have the application fully functional in a fraction of the time. As an added benefit, the software deployment tool will have updated the configuration management database automatically.

The differences in the outcomes of these two scenarios can be summarized easily; the latter situation offers:

- Reduced time to diagnose the problem
- Reduced down time
- Greater operational efficiency
- Reduced demand on service desk resources

The apparent payback of an investment in infrastructure management tools is not limited to anecdotal evidence or illustrative examples. Automation provides potential efficiencies in asset management that can reduce the TCO, and studies have verified this outcome:

- 90% reduction in the manual asset inventory activities according to EDS Labs
- 55% reduction in time spent on desk-side visits for hardware problems, according to Atos-Origin Labs; a similar evaluation from EDS Labs found a 50% reduction in desk-side visits
- 83% reduction in time spent on desk-side visits for software problems, according to Atos-Origin Labs; a similar evaluation from EDS Labs found a 50% reduction in desk-side visits
- 75% reduction in time-to-recovery values from 1 day to 2 hours, according to an EDS Lab evaluation

(Sources: "Improving IT Services and Increasing User Uptime with Intel vPro Technology," Atos-Origin Lab; "Improving Asset Inventories and Reducing IT Costs with Intel vPro Technology," EDS Lab.)

Substantial savings such as these are realized by combining detailed and up-to-date information about assets with tools for remotely delivering and administering software applications. Fortunately for enterprises planning Vista migrations, the migration is an ideal time to introduce such asset management tools.

### **AUTOMATED ASSET MANAGEMENT**

Throughout a number of steps in a Vista migration, information is gathered about the hardware, software, and configuration of devices. This information is then saved in a configuration management database—a centralized repository of information about hardware, software, and configurations deployed throughout the organization. After the migration, this same information is available to

- Lower costs by reducing the time required to diagnose problems, plan redeployments, determine licensing requirements, assess compliance, and a host of other common IT management tasks.
- Improve service by providing fine-grained, up-to-date information to service desk technicians as well as various levels of management detail for planning operations.
- Provide a more detailed, up-to-date view of the state of client infrastructure, which can be essential for mitigating emerging security threats and identifying vulnerable devices. Coupled with automatic patch deployment, this information can contain or even prevent security breaches.
- Enforce policies related to compliance and security management issues.

Detailed asset information can lead to even greater efficiencies when coupled with remotely managed hardware.

## **MAXIMIZING LONG TERM BENEFITS WITH INTEL VPRO PROCESSOR TECHNOLOGY**

A well-managed configuration management database contains a wealth of information for IT support staff, but combining asset management with the remote management capabilities of Intel vPro yields even greater benefits. Altiris asset management systems leverage Intel vPro capabilities for a wide range of systems management tasks:

- OS deployment and patching
- Network traffic filtering
- Power management
- Inventorying assets

A variety of studies have confirmed significant reductions in time and desk-side visits when Intel vPro processor technology is introduced:

- According to an Atos-Origin Lab study, critical patches applied to PCs with Intel vPro processor technology can reduce vulnerability windows by 30 times.
- An IT@Intel case study found hardware failures, which account for 35% of service desk calls, require two or more desk-side visits to diagnose and repair hardware failures; with Intel vPro, the problem can be diagnosed remotely and repaired with a single desk-side visit.
- The same case study found OS-related failures, which account for 19% of service desk calls, can be remotely diagnosed and repaired without a single desk-side visit.
- Providence Health Systems, Portland found Intel vPro processor technology reduced hardware repair times by 37.5% and software repair times dropped by 33%.

(Sources: "Improving IT Services and Increasing User Uptime with Intel vPro Technology," Atos-Origin Lab; 2003 Intel Trouble Tickets, IT@Intel; "Providence Health Systems Final Report," Intel Solution Services.)

The combination of Altiris automated management software and Intel vPro hardware can substantially increase the efficiency of asset management resulting in key benefits to IT operations:

- Reduced maintenance costs
- Improved service to customers with greater uptime and reduced troubleshooting times
- More detailed, up-to-date view of the state of assets
- Greater support for policy enforcement and security management

## Summary

A Vista migration presents an opportunity to introduce automated asset management tools and best practices. The Altiris 6-Step Process not only provides a managed framework for upgrading OSs, it is the start of a long-term asset management process. Altiris' centralized and automated asset management systems collect and manage detailed information about PCs, enabling IT staff to more effectively and rapidly respond to the needs of their customers. The remote management features of Intel vPro processor technology combined with Altiris' automated management bring even greater efficiencies, allowing organizations to reduce the costs of operations and maintenance and free resources for new, innovative initiatives.

---

Intel® Active Management Technology requires the computer system to have an Intel(r) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup of Intel AMT requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications or implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see [www.intel.com/technology/platform-technology/intel-amt](http://www.intel.com/technology/platform-technology/intel-amt).

Copyright © Symantec Corporation 2007. All rights reserved. Symantec, the Symantec logo and Altiris are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Intel, Intel vPro and Centrino are trademarks of Intel Corporation in the U.S. and other countries. Other names may be trademarks of their respective owners.