Migrating to a new client OS can be intimidating. Organizations want to take advantage of the productivity, security, and control enhancements in Microsoft Windows 7—but at this scale, how can they keep the migration efficient, cost-effective, and sustainable while helping ensure end-user productivity?

Symantec and Dell can help meet this challenge—and capture the opportunity. The seven-step process outlined in this article can provide organizations with a basis for developing their own thorough strategies to help ensure a successful migration. By following best practices and taking advantage of joint migration and management solutions like the Dell Management Console for Clients (formerly Dell Client Manager), they can streamline processes to help reduce the expense, delay, and disruption of a migration and keep IT administrators in control. And when these savings are applied to solutions for security, virtualization, data protection, and management, organizations can help secure not only the onetime rewards of a smooth migration, but also the long-term reliability, productivity, and security of an up-to-date, efficient, manageable IT environment.

**GETTING STARTED**

Before IT administrators can assist their organizations with a successful Windows 7 migration, they must understand what lies ahead and then formulate an appropriate plan. As they prepare, they should work to ensure that their team is ready by considering the following factors:

- **Communicating**: A successful migration involves coordination across the organization. Organizations can begin by assembling a team that represents key stakeholders, such as IT operations, security operations, application testing and packaging, network administration, and procurement.

- **Setting expectations**: Even a good process can be considered a failure if expectations are not met. As administrators formulate their migration plan, they should work with key stakeholders to understand their objectives and set achievable goals.

- **Identifying targets of opportunity**: Administrators should look for ways to take advantage of the migration. They may find ways to enhance and automate processes or address current objectives, such as standardization or compliance. Some enhancements to consider include standardizing software versions, consolidating software licenses, resolving security vulnerabilities, implementing information management technologies to back up data, and evaluating software delivery alternatives such as application virtualization and streaming.

- **Staying focused**: Migrations present natural opportunities to improve, but administrators should...
beware of out-of-scope distractions like network upgrades. Staying focused on migration-related projects helps avoid rising costs and scope creep, which can jeopardize success.

PHASE 1: PLANNING AND ASSESSING
In this initial phase, administrators assess resources and plan their migration strategy. This phase provides the foundation for the deployment plan, including the evaluation of hardware and software in the environment.

Step 1: Assessing the environment and planning the deployment
Gathering real information about the hardware, applications, and network in the environment helps administrators determine when to perform the migration and identify required resources. During this first phase, administrators assess the environment and outline the case for deployment and migration.

The assessment plan should include real information about the systems in the environment as well as key details about those systems, such as hardware and applications. Therefore, administrators should first discover devices across the network and run an inventory scan. This step helps identify the potential costs and risks of migration; otherwise, it can be difficult to prioritize or time the migration appropriately, and can be difficult to gather the necessary resources for a smooth and effective migration.

The next step is to assess hardware and software readiness. Organizations often use an OS migration as a time to evaluate the hardware, applications, software, and other aspects of their environment, as well as to plan for the future. Using preconfigured reports to identify hardware that requires replacement and evaluating what software is necessary are critical planning steps. Several of these reports are available as complimentary downloads for the Dell Management Console for Clients (see Figure 1).

After identifying applications that require migration, administrators must prioritize applications to test and migrate—beginning by identifying the applications that can run on Windows 7, which can be essential for system stability, security, and overall productivity. Because organizations may have hundreds or even thousands of applications, categorizing the applications by rank (critical to not important) and type (commercial, legacy, or custom) lays the foundation for testing priority. Administrators should begin with business-critical applications and work down to the least important. They can then map out a strategy for updates or replacements that may be required. Organizations should also familiarize themselves with options such as application virtualization that may be appropriate for some applications.

Having gathered the list of required hardware, software, and tasks required to complete the migration, administrators can then analyze overall migration costs and dependencies, starting with creating a time estimate for each task. The actual list of tasks is specific to each organization, but the steps described in this article can provide a good starting point. When identifying conditions specific to the organization’s environment, administrators should create a plan for dealing with these conditions as well as possible side effects from workarounds. Handling some dependencies could require additional time and resources, so advance planning can help reduce frustration and lost work later.

Finally, administrators should identify potential risks. The key elements affecting migration success are scope, time, and money, so before performing a full rollout, they should perform an analysis to identify risks that may affect these elements. These risks typically fall into one of four categories; Figure 2 shows some examples of possible risks that administrators should be aware of when planning a migration.

PHASE 2: DESIGNING AND BUILDING
During the second phase, administrators prepare for the migration by building standard images, preparing and testing applications, capturing user settings and personalities, and assembling and automating the migration process.

Step 2: Building standard images
Deploying a standard hard disk image is typically the fastest and most consistent way to install an OS. Symantec software
enables administrators to use the Symantec Ghost™ format or the Microsoft Windows Imaging (WIM) format, depending on the needs of the specific environment. Administrators can also choose to create a single hardware-independent image or to build and maintain a small set of base images.

When building a base image, administrators should start with the most common type of system on the network. They may also wish to use a virtual machine that has the ability to make snapshots and revert to those snapshots easily; during many of the planning and testing steps, it can be helpful to revert to a previous snapshot without needing to create and deploy image files. If desired, this base image can be built in a manner that allows it to be hardware independent.

As a best practice, administrators should typically keep images as small and generic as possible. In the base image, they should include only those applications that must be installed on all systems, and then install other applications in the same job but separately from the OS image. Certain applications may need to be installed on all client systems and therefore should be installed in the base image. However, administrators should keep in mind that because the base image is deployed to all systems, it could cause license compliance problems if a limited number of software licenses are available.

After installing all applications to be included in the base image, administrators should take another snapshot of the client system. They should not overwrite or replace the first snapshot that was taken—instead, they should keep two snapshots, one with only the OS installed and one with all base software installed. The second snapshot can be useful when testing other software installation packages to be installed after image deployment. It can also be used if there is a need to re-create the generic image.

**Step 3: Preparing and testing applications**

Applications that are not installed on the base image must be installed after the imaging process. Some of these applications may be installed as part of the migration process, while others may be installed later as users request them. Altiris Deployment Solution™ integrated migration software from Symantec works with Wise Package Studio™ and Symantec Workspace Virtualization software to package and virtualize applications.

Administrators should be sure to identify applications supported on Windows 7. In particular, a key step in the migration is to identify the business-critical applications that will be used in the Windows 7 environment that are not included in the master image, but will be deployed to each new Windows 7-based system.

To help identify applications that must be prepared for installation on Windows 7, administrators should classify the applications in their environment by first ranking them in order of importance—for example, critical, important, useful, or not important. They should also classify applications by type; Figure 3 shows an example of this kind of classification. Classifying each application is useful when determining steps for remediating application issues.

Many commercial applications have updates that are fully compatible with Windows 7; however, some software that has not been updated may have compatibility issues. After administrators have identified which applications they will need to install on Windows 7, they can begin testing those applications for compatibility. Software incompatibility is usually caused by one of the following:

- OS requirement
- Hard-coded path
- Requirement of administrator rights
- Class identifier (CLSID) registration in the registry
- File copy (rights or access control lists)
- Platform-specific drivers

Some applications may install and function correctly only when they are the sole application installed on a clean system, so it is important to test groups of...
applications that would commonly be used together on a single system to help identify potential risks. These issues are typically much easier to deal with at this stage rather than later in the migration process.

**Step 4: Capturing user settings and personalities**

During a migration, administrators should not forget that end users often dislike change. They want to start up their computers and see exactly what they expect—the same printer and network settings, background pictures, Internet favorites, and everything they have personalized in their most-used applications. A successful Windows 7 migration should minimize disruption to end users: the transfer of each user’s network, OS, application, and data settings along with other customizations can make or break a migration. Capturing these settings and applying them to the Windows 7 environment is necessary to maintaining productivity and accelerating acceptance.

Creating a personality template can help with this process. Altiris Deployment Solution from Symantec contains a Template Builder feature that enables administrators to define a common template that captures global settings, application settings, and data files (see Figure 4). The template specifies which settings to capture. It also provides a list of desktop and network settings, displays a list of over 60 common application components that transfer application settings and data files, and provides the ability to capture files and folders on the source system.

**Step 5: Assembling and automating the migration process**

After they have built and tested the required files and tasks, administrators must encapsulate them into a job sequence to help ensure that when one task completes, the next is triggered automatically. The automated migration process should include capturing personality settings (using the template created in step 4), deploying the OS image (using the image built in step 2), installing the required applications (using the applications prepared in step 3), and restoring the personality settings.

**PHASE 3: EXECUTING AND REPORTING**

An OS upgrade can be exciting for any organization—but if the anticipation leads to an attempt at immediate adoption without first testing the deployment process, that haste can cause significant problems. If the process encounters complications or other issues, then going straight to implementation becomes not a shortcut but a shortfall.

This final phase leads to the production rollout. It begins with a small-scale test and pilot. Administrators then implement the migration infrastructure designed in phase 1. Finally, they perform the production rollout and create migration reports.

**Step 6: Migrating systems**

Now that the planning has been completed, it is time to test and adjust the processes for deployment. The first step is to identify pilot or test candidates. Administrators can choose from several approaches to identify these candidates, and can also use these approaches to determine the pilot phases and subsequent migration rollout. Common migration approaches are shown in Figure 5.

Next, administrators should document the test cases. They can start by identifying the expected outcome of the migration job, including considering questions such as the following:

- Which applications should be installed?
- Which personality files and settings should be migrated?
- Which operating systems should be able to migrate using this process?
- Which computer models should be able to migrate using this process?

Based on these objectives, administrators can then create and document test cases to verify the success of each migration scenario. They can organize these cases...
into a test matrix to use for project approval and tracking.

After thoroughly testing the entire migration process on a single computer, administrators should next conduct a phased pilot migration, which gives an opportunity to test overall processes. They should start with a small group of carefully selected users as the target group. Best practices recommend running the first pilot on a small IT group that has been involved with the overall migration project, which provides a group that can understand when there is a problem and rapidly provide feedback to the project team.

When this first phase is complete, administrators should verify that data and settings have migrated as expected. Assuming the migration is successful, they can then move to the second phase of the pilot, which involves migration of the remainder of the IT department. Specific systems may need to be removed from the target list because those systems support critical applications or other critical systems.

The third and final phase of the pilot is to select a department that can be migrated. If this third phase is successful, the pilot phase ends and the full migration rollout can begin. Depending on the total number of managed clients and the complexity of the environment, this rollout may need to be performed in phases. There are various methods of phasing a large-scale deployment, so administrators should use the techniques appropriate to their environment.

The deployment process takes multiple steps, and complications can arise at each stage. A common approach is to start by migrating a small number of local systems in a single subnet or network, and complete the entire migration process on those systems. If a problem occurs, administrators may need to break apart the tasks that are contained in the migration job and run them separately on the systems being migrated, which enables them to analyze and identify the cause of the migration failure before increasing the number of systems migrated in the next group.

**Step 7: Measuring and reporting**

Effective reporting enables the organization’s executive team to track the migration from a distance while also helping IT administrators analyze different aspects of the migration. Key stakeholders may want to know the total number of clients running the new OS—or, more important, they may want to know which systems have not been migrated and what is being done about them.

Upper management is likely to value a formal return-on-investment study, which offers a prime opportunity to illustrate how proper planning, standardization plans, and automation helped accelerate the project and save money. Some key questions in this type of study include the following:

- What were the costs for rolling out an OS before this project?
- What tools provided the best help to automate the process?
- How much did the organization save in terms of capital expenditures and reduced resources?

**ENABLING A SUCCESSFUL MIGRATION**

Symantec and Dell provide an integrated set of solutions to help streamline a migration, including the Dell Management Console for Clients (which enables administrators to quickly assess their ability to migrate to Windows 7) and Altiris Deployment Solution from Symantec (which helps them to automate and streamline the migration for optimal savings and long-term benefits). Taking advantage of these tools, adhering to migration best practices, and using the seven steps in this article as the basis for a thorough migration strategy can help ensure a successful migration while enabling organizations to begin gaining the long-term benefits offered by the Windows 7 platform.

Christine Ewing is the director of product marketing in the Symantec Endpoint Management Group, and has more than 12 years of experience in IT software product management and marketing.

John Stahmann is the technical alliance manager for the Dell Alliance team at Symantec, and has more than a decade of experience with systems management and Microsoft Windows migrations.