

7 Steps to Windows 7

Migrating with Altiris™
Deployment Solution 6.9 SP3
from Symantec

7 Steps to Windows 7

Migrating with Altiris™ Deployment Solution 6.9 SP3 from Symantec

Contents

Migrating with Symantec Solutions	1
General Migration Guidelines	2
7 Steps for Windows 7 Migrations	2
Assess and Plan	3
Step 1: Assess Your Environment and Plan Your Deployment	3
Build and Test	10
Step 2: Build Standard Windows 7 Images	10
Step 3: Prepare Applications	12
Step 4: Capture User Settings and Personality	15
Step 5: Assemble and Automate	20
Execute and Report	23
Step 6: Migrate Systems	23
Step 7: Measure and Report	26
Additional Windows 7 Migration Information	27
Appendix A	28
Appendix B	30

Migrating with Symantec Solutions

Migrating to Microsoft Windows 7 can be an intimidating task. You want to take advantage of how Windows 7 will help make users productive anywhere with enhanced security and control, but how do you implement an efficient, cost-effective migration that doesn't disrupt end-user productivity? While challenging, migration also presents an opportunity. It's the perfect time to wipe the slate clean; to implement standard configurations and structured change management procedures that will help ensure the long-term rewards that come from a manageable, sustainable environment.

Symantec has migrated more than 300 million desktops and notebooks to Windows 2000, XP, Vista and now the Windows 7 operating system. With more than a decade of experience, Symantec's expertise is engineered directly into our solutions. Combine the expertise with our powerful hands-free, fully-automated technology helps customers simplify a seemingly difficult hardware refresh or OS migration.

Why Use Symantec for Your Windows 7 Migration?

Integration - Symantec solutions not only deploy the OS image. They perform inventory and assessment, virtualize applications, capture application settings and user data, conditionally install applications based on the user or department, and reconfigure the migrated computer-all from a single console. This integrated, automated approach eliminates the need for custom scripting, and ensures that when the migration finishes the machine is ready to use, eliminating hundreds of hours in unnecessary help desk support calls.

Automation - Symantec customers have migrated millions of computers to new operating systems using a single job and a single hardware independent image. Most organizations don't have the time or personnel to manually perform each part of a migration, so we've designed our tools to fully automate the process, allowing you the option to remotely carry out full migrations without even touching the computers being migrated.

Proven technology - Symantec provides native support for sector-based imaging as well as the new WIM image format introduced with Vista. Your migration starts from wherever you are at-even Windows 98, 2000, XP, or Vista machines. We believe that your technology decisions should be based on business needs, not the limitations of your software.

As the key deployment partner for desktops, notebooks, workstations, thin clients, and servers for Dell, HP, Fujitsu Siemens Computers and IBM servers, Symantec works closely with all major hardware manufacturers. We also support hardware-based management technologies such as Wake on LAN, PXE, and Intel® vPro™, ensuring you can take full advantage of hardware features.

Post migration management - as part of a migration project, you will be building all of the pieces (standard images, software packages, etc.) necessary to put an on-going management system in place. Symantec solutions allow you to leverage this investment and to continue to secure and manage your IT resources long after the migration is complete.

General Migration Guidelines

Having a sound migration plan and an integrated, automated solution is important for migration. Making sure your team is prepared can be just as important. As you prepare for Windows 7 migration, be sure your team is ready.

Communication - a successful migration involves coordination with people across your organization. As part of your migration plan, identify who within your organization will need to see and/or approve various aspects of the migration, and make a plan for how you will make sure they are informed and involved at the right time.

Set expectations - even a good process can be considered a failure if expectations are not met. As you make your migration plan, work with key stakeholders to understand their objectives and to make sure that you are setting achievable goals.

Identify other opportunities - as you work through your migration plan, look for ways to take advantage of the migration to improve and automate processes or address current objectives in areas such as standardization, automated management, compliance and security. Some improvements you might want to consider include:

- Implement computer naming standards
- Standardize software versions
- Resolve security vulnerabilities
- Harvest and consolidate software licenses

Stay focused - Migrations present natural opportunities to improve. However, be sure to avoid distracting out-of-scope projects, such as network upgrades. By staying focused on projects related to the migration, you can limit cost and scope creep that might ultimately jeopardize your success.

Prerequisites to Windows 7 Migration

- Install Deployment Solution 6.9 SP3
- Create the Automation boot environment so it is ready to boot clients

7 Steps for Windows 7 Migrations

Successful migration is only possible with a thorough strategy. We have used our years of expertise to develop the Symantec 7 Step Windows 7 Migration process.

This process includes three phases:

- ◆ Assess and Plan
- ◆ Build and Test
- ◆ Execute and Report

Assess and Plan

In this initial phase, you will assess resources and plan a strategy to ensure a successful migration. This includes evaluating the hardware and software in your end user environment, and identifying network and management issues across your organization. Symantec solutions help with assessment and planning by providing pre-built reports. These reports enable you to determine hardware readiness and overcome infrastructure barriers to ensure a smooth migration. This assessment and planning phase provides the foundation for your deployment plan.

Step 1: Assess Your Environment and Plan Your Deployment

Gathering real information about your hardware, software applications, and network will help determine when to migrate and what resources are required for the migration. Is your network ready for a large-scale rollout? Evaluating your organization's physical requirements and topology is the key to developing an accurate and predictable deployment plan. During this phase you will assess your environment as well as outline your deployment and migration business case by doing the following:

- ◆ Discover devices across your network
- ◆ Run an inventory scan
- ◆ Assess hardware readiness through reports
- ◆ Assess software readiness to prioritize applications to test and migrate
- ◆ Determine where and how you will utilize multicasting and local file shares
- ◆ Add costs, timeframes, and required hardware and personnel requirements to plan
- ◆ Determine dependencies unique to your organization
- ◆ Develop acceptable Service Level Agreements (SLAs)
- ◆ Create communication plans
- ◆ Identify potential issues and risks

Discover Devices Across Your Network

The first step in analyzing client systems in an environment is to actively manage endpoints with client software. Altiris Deployment Solution uses AClient and DAgent to manage client systems. AClient is installed and used on client systems with Windows XP and older Windows operating systems. DAgent is used for Windows XP and newer operating systems. Since each agent contains the same functionality it doesn't matter which is used with Windows XP.

There are a variety of methods to install the agent on each end point. Depending on your network infrastructure or personal preferences choose from one of the following:

Remote Agent Installer - This is usually the preferred method to install the Deployment Solution agents. This program can be accessed from the Deployment Solution Win32 console from *Tools > Remote Agent Installer*, or it can be accessed from the Deployment (eXpress) share with the file *rcinstall.exe*. The wizard will ask you for agent settings, and a user account used to access the systems remotely.

This utility requires that each endpoint has remote file system access, remote registry, and remote services access. If this utility is failing to install the client software on an endpoint you can attempt the following three tests. Try to map a

7 Steps to Windows 7

Migrating with Altiris™ Deployment Solution 6.9 SP3 from Symantec

network drive to \\clientComputerName\c\$. Open up regedit.exe and select *File > Connect Network Registry* and attempt to connect to the client system's registry. Open up Windows Services (services.msc) and from that dialog select *Action > Connect to another computer* and from there attempt to connect to the remote system's services.

AD group policy - If the Remote Agent Installer cannot be used for some reason, and all client end points are joined to a domain, group policies can be used to install the Deployment Server agent to end points. The installation of AClient or DAgent can be done in a batch script that can then be run from a domain group policy. More information about this process can be found in [Altiris KB Article 1680](#).

Other endpoint management system - If endpoints are already managed by a desktop lifecycle management product, such as Altiris Client Management Suite, it can be fairly easy to create a package and push out the agent with that software. Since this is different for each type of management software you will need to reference the product documentation. [Altiris KB Article 45334](#) explains the process with Altiris Client Management Suite.

Manual installation - A manual client installation might be preferred if no remote installation option will function or if the number of remote endpoints is very small, such as in a test environment. From the client computer, browse to the eXpress share and copy over to the client system AClient.exe or DAgent.msi (depending on the client operating system) and then run the file. Both of these contain a short installation wizard which will prompt for agent settings, such as installation directory and Deployment Server IP address.

Run an Inventory Scan

As soon as a Deployment Solution Agent is installed to a client machine, it begins sending basic inventory, such as computer name, network information, domain information, and basic hardware information. Basic inventory is sent every time the Agent connects to Deployment Server. The Agent also sends full inventory such as detailed hardware information, services, applications, etc. Full inventory is sent at a configurable interval which is every 24 hours by default. If you want to make sure that a particular report contains the latest inventory data, you can schedule a Get Inventory task to all computers to force a full inventory scan.

This information is stored in the Microsoft SQL server specified during the Deployment Solution installation. The Deployment Solution Win32 console has the ability to view detailed inventory for a single client system. It does not have a method to generate reports or view groups of inventory data in a spreadsheet. Other tools will be required to generate these types of reports.

Various tools are available to generate these reports such as Microsoft Report Builder or Crystal Reports. SQL Management Studio also has query analyzers that allow simple query results from a SQL query. All of these tools use Transact SQL (or TSQL) as the basis of building these reports. A basic understanding of the Deployment Solution database schema is required to generate reports and gather needed data to perform proper analysis. See Appendix A for information about the data stored in the eXpress database and sample queries that can be used to retrieve that information.

Assess Hardware Readiness through Reports

You will need to query your Deployment Solution database to generate a list of client computers that meet the following requirements:

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)
- DirectX 9 graphics device with WDDM 1.0 or higher driver
- More information can be found at <http://www.microsoft.com/windows/windows-7/get/system-requirements.aspx>

You can get this list by running the following query against the Deployment Solution Database:

```
SELECT C.name, H.proc_speed, H.ram_total, CASE proc_type WHEN 1 THEN 'x86' WHEN 2 THEN 'x64' ELSE 'incompatible'  
END AS architecture, D.name AS [graphics device name], D.manuf AS [graphics device manufacturer] FROM computer C,  
hardware H, device D WHERE C.computer_id = H.computer_id AND C.computer_id = D.computer_id AND D.class LIKE  
'%4d36e968-e325-11ce-bfc1-08002be10318%'.
```

Assess Software Readiness to Prioritize Applications to Test and Migrate

The Deployment Server database will contain all applications that are installed on client systems, provided that the application registers itself with the Windows operating system (i.e. the application is displayed in Add/Remove Programs). After the Deployment Solution Agent is installed on all client systems that will be migrated, a report can be built that will give a list of all software currently installed. Some of this software might not be supported by your IT group, but it should provide a good list to work from to build a list of applications that will be installed during or after the Windows 7 migration process.

Query your eXpress database to generate a list of all software in your environment that will be included in the Windows 7 Migration. This information can be queried from the Applications table in the eXpress database. When you have the list, check with the application vendors to determine what applications are Windows 7 compatible.

You can get this list, sorted by the count of computers having that application, by running the following query against the Deployment Solution Database:

```
SELECT COUNT(1) AS [count], [publisher], [description], [name], [version], [product_id] FROM [application] GROUP BY  
[publisher], [description], [name], [version], [product_id] ORDER BY [count] DESC, [publisher], [description], [name].
```

Determine Where and How You Will Utilize Multicasting and Local File Shares

Out of the box, Deployment Solution supports three imaging engines: RDeploy, Ghost, and ImageX. Before determining where and how to use multicasting and local file shares, it is important that you understand the difference between these imaging engines and how it affects you.

RDeploy - This is the native imaging engine in Deployment Solution 6.x. It is the only imaging engine that uses multicasting technology to reduce server load while deploying the same image to many clients on the same subnet. RDeploy supports most drive formats, including FAT, NTFS, and EXT3.

Ghost - This is the native imaging engine in Deployment Solution 7.x. It does not support multicasting. Ghost supports most drive formats, including FAT, NTFS, and EXT3. It supports preserving specific files and folders while deploying a new image to an existing system.

ImageX -This imaging engine was developed by Microsoft. It does not support multicasting. ImageX only supports the Windows compatible driver formats FAT and NTFS. With some customization, you can preserve specific files and folders while deploying a new image to an existing system.

	RDeploy	Ghost	ImageX
Multicast	X		
FAT	X	X	X
NTFS	X	X	X
EXT3	X	X	
File Preservation		X	X

A powerful use of Ghost's file preservation is during personality capture and deployment during an in-place migration. When performing in-place migration (the same hardware to a new operating system), you can store the personality package on the hard drive rather than the file server. Since personality packages have the potential to become very large (sometimes in the gigabytes), the file preservation technique will speed up the migration and reduce server workload. Since no imaging engine supports both multicasting and file preservation, you need to determine which feature will benefit you the most. If you choose to take advantage of this feature, make sure to capture your images as Ghost (GHO) files.

Large and complex networks are going to require a lot of work to determine how replication and imaging will be done. If a large number of imaging tasks are going to run simultaneously, multicast research should be done. If PXE will be used then DHCP infrastructure and IP helpers need to be considered.

Image Placement and Management - In segmented networks across a WAN it is important to place image shares at each LAN location and identify what the link speeds from each image share to the endpoints. You will need to test network transfer speeds between the end clients and the file shares. It is important to test a variety of clients to identify potential weak or trouble spots that could cause problems. If necessary a single LAN site might need more than one local file share, or perhaps a single file share could be used across multiple LANs. The requirements for a file share are fairly simple, a Windows system, sufficient resources (such as disk space and network access), and high availability.

Once local file share needs have been identified, order any new server hardware that is deemed necessary and position them at their respective places in the network.

Multicast and Broadcast domains - Deployment Solution utilizes both multicasting and broadcasting for various functions. It is important to determine where broadcast and multicast boundaries exist, and if multicasting (or IGMP) is enabled on your network devices (usually at the switch level). Broadcast technology is used with both PXE (Pre-boot eXecution Environment) and WOL (Wake On Lan). These are both very useful tools used for image deployment, but are not required. Since broadcasting is often very restricted in most networks, certain accommodations need to be made to allow the use of these functions.

PXE Broadcasting - The PXE pre-boot technology allows a client machine to boot to a pre-boot environment, such as WinPE or DOS, without using any physical media at the client system, such as a boot CD. It does not utilize the hard drive while booting, so it is ideal for zero footprint provisioning. PXE utilizes the same network protocol as DHCP. Since a client's PXE boot behavior is dictated by the BIOS boot process, and by the Intel PXE boot protocol standard, it cannot be configured or modified.

PXE clients send broadcasts on UDP port 67 and receive a response on UDP port 68. Normally broadcast packets on these ports are forwarded to the DHCP server even if they are across broadcast domains. If client machines are on a separate LAN from the PXE server and the UDP broadcast packets cannot get from the client machine to the PXE server due to network design, one of the following three things will need to be done to use PXE:

1. Install a secondary PXE server at each local LAN in each broadcast domain.
2. Use/add IP helpers on network devices (generally routers) to forward DHCP packets to the IP address of the PXE server.
3. Add DHCP scope options to the DHCP server. This is known as using PXE Forced Mode.

Adding a PXE server to each LAN is a good idea if each site is a very long distance, or has a slow link between each link. If a very large number of LAN sites exist it can cause complexity very quickly. Generally if a small number of remote sites (such as 5 or less) are being used then this method is fairly easy to implement. In very large environments where hundreds of sites exist it is not recommended to use this method.

Adding IP helpers to all network devices can be a challenging unless a replication method is in place by the network administration team. Depending on the difficulty of modifying and maintaining the network infrastructure this method can be investigated. Adding IP helpers also increases the amount of network traffic going across broadcast domains. This

additional traffic needs to be monitored to determine if it will cause network congestion or other complications. If the network in general does not have very much DHCP traffic, then this change should not have very much impact over all.

If the DHCP server scope options are available for modification it is highly recommended to use scope options to redirect clients that are PXE booting from the DHCP server to the PXE server. Using this option requires an understanding of DHCP scope options. The [Altiris KB Article 33999](#) explains how to configure these scope options on a Microsoft DHCP server.

If you are using a non Microsoft DHCP server the same DHCP options/principles can be applied with slight modifications. Instruction for certain popular DHCP devices may be found in the Altiris Knowledgebase.

Add Costs, Timeframes, Hardware, Software, And Personnel Requirements To Plan

To determine the costs, timeframes, and personnel requirements you will need to make a list of required hardware, software, and tasks to complete the migration. When you have the list, you can then add time estimates for the tasks. Then, estimate the cost for the hardware, software, and estimated task time requirements. The list of tasks will be unique to your business, but a good place to start is the tasks outlined in the table of contents of this document.

When you have determined the tasks and the time required for each task, you can then determine which tasks will need multiple staff and designate who will be working on each task.

Determine Dependencies Unique To Your Organization

Each organization has its own unique requirement and dependencies that need to be addressed before a full rollout can be accomplished. It is important to identify these requirements during the initial pilot rollout or perhaps even earlier. Some of these might include:

- Blackout times where productivity cannot be impacted by downtime.
- Total network bandwidth that is available.
- Impact on network applications and interruption of network services caused by:
 - A large amount of imaging
 - Transferring large files
 - Personality migration
 - Remote application installations

When identifying these unique conditions in your environment make a plan on how these will be dealt with as well as possible side effects of any workarounds. If these items will delay a full rollout then the estimates created in previous stages need to be updated. Some of these dependencies could add time and resources. Planning for dependencies ahead of time will reduce frustration and lost work.

Develop Acceptable Service Level Agreements (SLAs)

At this point, you know how many people will be working on each task. You can use the time required for each task divided by the number of staff working on it to determine how many work hours each task will take. You can then determine how many days each of the 7 steps will take and declare a target date to have each step completed.

Create Communication Plans

You need to create a communication plan document that describes:

- Your objectives
- How you will accomplish the objectives
- Who will be notified of status updates
- When status updates will be communicated
- Timetable
- Reports

Identify Potential Issues And Risks

Factors of a successful project are scope, time, and money. Prior to a full rollout of Windows 7 Migration, analysis needs to be done to identify potential risks that may affect these factors. These risks will fall into one of four categories. Here are some examples of possible risks (this is not an exhaustive list):

1. Technical, quality and performance
 - Unforeseen environmental dependencies
 - Data loss
 - System outages
2. Project management
 - Timelines are not met
 - Inadequate project plan
3. Organizational
 - Lack of resources
 - Inconsistent objectives or project scope
 - Poor prioritization
4. External
 - Power outages
 - Legal issues
 - Labor issues
 - Changing priorities or expectations

Build and Test

During the second phase, you can prepare for migration by building image files, identifying application compatibility issues, building application packages, and generating personality templates. You will also build and test your migration workflow job to ensure all files and templates are in place and ready to go.

Step 2: Build Standard Windows 7 Images

Deploying a standard hard disk image is the fastest and most consistent way to install a new operating system. Symantec allows you to use our Ghost or Microsoft's WIM image format, depending on what makes sense for your environment. You also can choose to create a single-hardware independent image, or build and maintain a small set of base images.

Depending on the complexity of your environment, a small set of base images may be most effective. As a best practice, keep images as small and generic as possible. Only include applications in the base image that must be installed on all computers, and install other applications in the same job, but separately from the OS image. Regardless of what image strategy you choose you will need to follow these steps:

- ◆ Create standard images with settings and configuration for multiple users
- ◆ Include applications that are required on all computers in the base image
- ◆ Create generic image

Create Standard Images With Settings And Configuration For Multiple Users

The first choice to be made when building a base image is what hardware to use for the client. One good approach is to use the most common type of system on the network. Another possibility is 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 phases it will be very helpful to revert back to a previous snapshot without having to create and deploy image files. If done correctly when the image is deployed, whichever hardware is used for the client system should be hardware independent.

Once the base operating system is installed it is important to make a snapshot of the system. This is not a snapshot that will be used for the migration process, and it is important that if you are building a Windows Vista or Windows 7 image that you make the snapshot without using Sysprep. This snapshot will be used when there is a need to revert back and reinstall base software on the image, or if modifications are needed but a clean starting point is wanted. This snapshot should include just the base operating system without any third-party software.

If you are using VMware, or some other PC visualization software creating a snapshot is a very simple built-in process. If you are using physical software you will need to capture an image file with RDeploy or Ghost. Manually boot the client machine into a pre-boot environment, such as WinPE or LinuxPE, and assign a job that captures an image without booting to Production.

Create a job in the Deployment Server console named "Create backup snapshot". Add a "Create Disk Image" task to the job. It is recommended to use a token in the image file name so that the job creates a separate image file for each client that it is run against. Depending on where images are stored the path will vary. If computer images are stored in the eXpress share in the images directory the image storage path might be .\Images\%COMPNAME%.img. Make sure that the

7 Steps to Windows 7 Migrating with Altiris™ Deployment Solution 6.9 SP3 from Symantec

check box "Prepare use Sysprep" is unchecked and also "Do not boot to Production" is checked. This will prevent clients from doing any type of image pre-configuration.

The difference between a basic snapshot image and a generic deploy-able image is whether any pre-configuration is done. When a generic image is created the agent installed on the client machine will run Sysprep which will force a Windows setup on the client, it will also remove it from the domain, pull out any network configurations, such as static IP addresses, static routes, etc. After a generic image is captured it can be deployed to multiple other systems regardless of their hardware or configuration. A snapshot image that is not made generic should only be used to restore a previous state on the same system the image was captured from.

Include Applications That Are Required On All Computers In The Base Image

Certain applications might need to be installed on all client systems. These should be installed in the base image, not on clients after image deployment. Identify what software is required for all client systems and what software will only be needed by some users. Take into account licensing required and any asset management that needs to be done. While it might be simpler to include all software into the base image, it might cause license compliance problems if a limited number of software licenses are available.

After installing all applications that will be included in the base image, it is highly recommended to capture another snapshot of the client system. Do not overwrite or replace the first snapshot that was taken. You will keep two snapshots, one with only the OS installed, one with all base software installed. The second snapshot will be useful when testing out other software installation packages that will be installed after image deployment. It can also be used if you need to re-create your generic image.

Create Generic Image

When the client system is set up with all software and configurations that are required for the base system you are now ready to create a generic image to be used for deployment. Before a generic image can be created you must have installed the Altiris Deployment Agent (Dagent.exe) on the client system. This agent will automatically run Sysprep and perform other image preparation tasks prior to imaging. When this agent is installed on the client system and reporting into the Deployment console, you are ready to proceed.

Create a job in the Deployment Console named "Create generic image" and add a "Create Disk Image" task to the job. In this job make sure that "Prepare using Sysprep" is checked, and that "Do not boot to Production" is NOT checked. Make sure that the proper operating system is selected and a valid Product key is selected as well. This will allow the client system after imaging to reapply its license, which is required after running Sysprep. When the job is created assign it to the client system while the client is currently in production and the Deployment Agent is actively connected to the Deployment Server and showing active in the console. You should see the client system run Sysprep, shut down, reboot into automation such as WinPE, and then start capturing the image with RDeploy or Ghost.

Windows 7 only allows the application of a license file up to 3 times. After this you will no longer be able to run Sysprep on that system. This is one of the reasons for creating a backup image that was captured without Sysprep. If you need to make changes to your generic image, revert to the image snapshot, make modifications, and then recapture the generic image using Sysprep.

Step 3: Prepare Applications

Applications that are not installed on the base Windows 7 image will need to be installed after the imaging process. Some of these applications will be installed as part of the migrations process and others might be installed later as needed. One major feature of Deployment Solution is the ability to deploy applications. It also works together with Wise SetupCapture and Symantec Workspace Virtualization (formerly Software Virtualization Solution) to package and virtualize applications. To prepare your applications for Windows 7 migration, you will:

- ◆ Identify the applications supported on Windows 7
- ◆ Test applications on Windows 7 and with each other to ensure compatibility
- ◆ Remediate issues through policies, packaging, virtualization, or code changes

Identify The Applications Supported On Windows 7

A key step in this Migration to Windows 7 is to identify the business critical applications that will be used in the Windows 7 environment that are not included in the master image that will be deployed to each new Windows 7 computers. The applications to be identified in this section are those that will be installed after the Windows 7 image has been deployed. Identifying can be a big task with the sheer number of different applications in the environment.

Classification of Applications-To help identify which applications need to be prepared for installation on Windows 7, classify them using the following list:

Rank

- Critical
- Important
- Useful
- Not important

Category

- Commercial Applications
 - Applications with broad distribution and current development by ISV
 - ISV's are working hard to update their applications
 - These applications are well represented in Microsoft Mitigation (ACT, Shims, and Community)
- Legacy Applications
 - Were developed by ISV's
 - Often business-critical
 - Not as well represented in MS Mitigation or community

- Custom Applications
 - Developed in house
 - Business Critical and represent unique challenges
 - Not represented by most MS Mitigation (other than detection). Not represented in community
 - Hard-coded paths in applications (Temp, My Documents, Documents and Settings, and Applications with platform specific drivers)

Refer to the list of installed applications you generated in Step 1. It is important to verify which of these applications will run successfully on Windows 7. Consult each software vendors support resources to validate support for that platform. It also might be useful to attempt to install and run each application on a test Windows 7 system to verify that basic functionality for each application is available.

Test Applications On Windows 7 And With Each Other To Ensure Compatibility

Much of this step will need to be done either through research via resources available by third-party software vendors or by manually testing software with a Windows 7 workstation. Many commercial applications have updates that are fully compatible with Windows 7; however some software has not been updated and might have compatibility issues.

After you have identified which applications will need to be installed on Windows 7, you can begin testing them for compatibility. First, check the software vendor website for information concerning Windows 7 readiness for each application. We recommend that you test the software in a lab environment.

Software incompatibility is usually caused by one the following:

- Operating System requirement
- Hardcoded path
- Administrator rights required
- Class Identifier (CLSID) registration in the registry
- File copy (rights)
- Applications with platform specific drivers

Be aware of these issues as you test each application. If an application fails, the reported error messages may correspond to one of these issues.

Manual Application Test - Follow these steps to test each application on a clean Windows 7 image (these steps may be different depending on the application requirements):

1. Revert to your Windows 7 clean image. Use the base image snapshot taken in step 2.
2. Install the application.
 - a. If requested for permission, click **Permit**.
 - b. If the application fails with no request for permission, right-click the installer and choose **Run as Administrator**.
3. If errors are reported:
 - a. Right-click the installer and click **Properties**.
 - b. Open the **Compatibility** tab.
 - c. Enable **Run this program in compatibility mode**.
4. When the install has completed, launch the application.
5. If the application does not launch:
 - a. Right-click the application icon and click **Properties**.
 - b. Open the **Compatibility** tab.
 - c. Enable **Run this program in compatibility mode**.
6. Verify the application performs properly. Perform use case tests to validate functionality.
7. If the application fails to function correctly, remediate the issues as explained in the next section.

Some applications will install and function correctly when they are the only software installed on a clean system. It is important to test groups of software packages that would commonly be used together on a single system to identify potential risks. Install various combinations of software that will be used in your production systems. It is much easier to deal with these issues now rather than later in the migration process.

Application installation with Deployment Solution - After you have validated that an application will install and function properly on Windows 7, you will need to create an installation package and job. Command-line parameters will be needed to perform an automated silent install using Deployment Server. Most software already comes with a method to install it silently, or with a silent installation answer file. Consult with the application vendor to find command line options for installation. Most MSI files will accept the following command: `MSIEXEC.EXE /I "installer.msi" /QN`.

More information can be found at <http://technet.microsoft.com/en-us/library/cc759262%28WS.10%29.aspx>.

Before you are ready to install an application using a Deployment Solution Job, you must be able to:

1. Copy the installer file, or a folder containing installer files, to the client computer.
2. Run a batch script or command.
3. Make sure the application installs without interaction.

Move the installation file or folder to the Deployment Server's eXpress share. You might want to consider creating a folder in the root of the eXpress share that will contain all software installation packages. From the Deployment Console create a new job. Add a "Distribute Software" task to the job. Browse out to the main executable or MSI file of the installation package. If the installation package uses multiple files, check the box **Copy all directory files**. Add the command line parameters under **Additional command-line switches**. Validate the software installation job by running it on a few Windows 7 test systems.

Remediate Issues Through Policies, Packaging, Virtualization, Or Code Changes

As mentioned earlier, Deployment Solution is integrated with Wise SetupCapture and Symantec Workspace Virtualization. These can both be used to help remediate issues with software installation. If the application is not business critical then you may want to wait for the software vendor to update the application to be Windows 7 ready.

Wise SetupCapture is a solution that will create an MSI package from a software install. SetupCapture will track any changes made to the system. It will then compile the changes into an MSI file that can be used to deploy the application. Additional information can be found in [Altiris KB Article 20052](#).

Symantec Workspace Virtualization also tracks changes made to the system, but it does not create an MSI package. It instead creates a VSA file which is considered an application layer. When a VSA layer is activated on a client system it appears that the software is installed and it is fully functional. However, files and registry keys have not been actually committed to the Windows operating system. Additional details can be found in [Altiris KB Article 40553](#).

Step 4: Capture User Settings and Personality

If there is one thing that will make or break an OS migration, it is the successful transfer of computer and user settings (network, operating system, applications, data, etc). To ensure a successful transition include:

- ◆ Global settings
- ◆ Application settings
- ◆ Data files
- ◆ Verify PCT Template

Global Settings

The PC Transplant (PCT) Template Builder lets a user define a template. A PCT Template specifies which settings will be captured during a Capture Personality task. The tool has an interface similar to the PCT Wizard. Because the tool is generic, a user cannot select a specific user's settings to migrate. The tool provides a list of all Desktop and Network settings. It does not include any system specific options like the listing of a specific printer.

Use the Template Builder to create a custom template for your organization. Your custom template will be used during the migration job discussed in the later sections.

7 Steps to Windows 7 Migrating with Altiris™ Deployment Solution 6.9 SP3 from Symantec

From the Deployment Server, open your PCT Template Builder. Note: The Template Builder can also be started by running Template.exe located in the PCT subfolder of your Deployment Share.

1. From the Deployment Console's menu bar, select **Tools > PC Transplant Editor**. The Explanation of utility and features dialog appears.
2. Mark **Don't explain again** and click **OK**. The Altiris PC Transplant Editor is opened.
3. From PC Transplant's menu bar, select **Tools > Template Builder**.
4. Select **Don't remind me again** to the update prompt and click **OK**. The PC Transplant Template Builder dialog appears as shown in the figure below.

You can use predefined templates or a custom template that you create. The following predefined templates are available:

- Default - Comprises of Desktop settings and a few Network settings such as the Folder/Driver share assignments, Dial-Up/RAS, and Windows drive mapping. No application, file, or data settings are captured by the Default.pbt.
- DNA - Comprises all Desktop, Network, and Application settings.
- DNMail - Comprises all Desktop, Network, Microsoft Outlook, and Microsoft Outlook Express mail settings.
- DNOOffice - Comprises all Desktop and Network settings, and all Microsoft Office applications settings.
- DNMSApplication - Comprises all Desktop and Network settings, and all Microsoft applications settings.
- DNLotus - Comprises all Desktop, Network, and Lotus application settings.

Continuing from the steps above, you should follow the steps below to complete the custom template:

1. Click **Next** to begin creating a new template.
2. Confirm that the **Create a new template from Predefined Templates** option is selected and that the Default.pbt default template is selected. If you have a custom template that was previously saved use it instead of the Default template.
3. Click **Next**. The User Capture Options dialog appears.
4. Select **Capture domain users**.
 - a. In the **Source** field type Your Domain\Administrator.
 - b. In the **Destination** field type Your Domain\Administrator.
5. Click **Add**. The user is added as shown in the figure below.
6. Click **Next**. The PCT Settings dialog appears.
7. From the **Desktop** page, complete the following:
 - a. Click **Clear All**.
 - b. Mark **Display Properties**.
8. From the **Network** page, select all the setting that you want to migrate for each computer.

Application Settings

The Template Builder tool displays a list of all applications supported by PC Transplant. The list is built using the current applications defined in the A2i files found in the PCT\?? folder (where ?? is the two character code for your language, such as EN for English). It also includes all the applications defined in .A2i files provided by the user in that folder.

The .A2i files are used to describe all the components that are needed to transfer an application's settings and data files. Each .A2i file is specific to a certain application and is used by the PCT Wizard to show the user which application settings can be migrated and how to collect this information.

1. From the **Applications** page, expand the Applications that you want to migrate and mark all settings.
2. Click **Next**.

Data Files To Migrate

The PCT template can specify the capture and migration files and folders that may exist on the source computer.

1. From the Files page, click **Add New**.
2. In the **File name** field, enter each file that you want to migrate and click **Open**. The Template Builder does not require the file to exist on the computer where the template is being built.
3. From the Folders page, click **Add New**.
4. In the Folder field, enter the name of each folder that you want to migrate and mark **Include Subfolders**.
5. Click **OK**.
6. Click **Next**. The Capture Options dialog appears.
7. Click **Next** to accept the default options. The Deploy Options dialog appears.
8. Click **Display Options** (in the upper right corner) and configure as follows:
 - a. Title: Type My Personality Package.
 - b. Description: Type Captures wallpaper and Internet Explorer settings. Use all other default settings.
9. Click **OK**.
10. Mark **Run Personality Package in quiet mode** and click **Run minimized**.
11. Click **Finish**. The Creating a Personality Build Template dialog appears.
12. In the **Save as** field, type the following destination path and name:
\\DSServer\Express\PCT\YourTemplateName.pbt
13. Click **OK**.
14. Click **Finish**. Your PCT Template, named MyTemplate.pbt, has now been created and saved in your Deployment Share's PCT folder.
15. Close the PC Transplant editor.

Verify PCT Template

Capture a Computer's Personality - The Capture Personality task allows the use of tokens (such as %COMPNAME%) when selecting the name of the package to be captured. This gives you the ability to use one task to capture the computer personality from many computers, with the result being unique and separate personality packages for each computer.

From the Deployment Console, create a new job in your My Jobs\PCT folder named Capture Personality.

1. Add a Capture Personality task to your new job and configure it as follows:
 - a. Personality template file: Type [\\DServer\Express\PCT\YourTemplateName.pbt](#)
 - b. Store package in folder: Type [\\DServer\Express\PCT\MyPackages](#)
 - c. User account and folder login
 - d. User Name: (select Administrator User)
 - e. Password and Confirm password: (password)
2. Click **Advanced** and select **Domain users and Local users**. These settings overwrite the equivalent setting created in the template.
3. Click **OK**.
4. Click **Finish**. Your capture personality job is now created.
5. Click **Yes** to confirm the creation of the new folder.
6. From the Deployment Console, schedule the Capture Personality job to run immediately on the some of your computers.
7. Look in the MyPackages folder and verify that the personality packages were created.
(\\DServer\Express\PCT\MyPackages)

Restore personality settings and data files - The Personality Package is a wizard-based self-extracting executable file. You can distribute a Personality Package by floppy disk, e-mail, network share, CD, or Web download. Personality Packages can also be deployed using Deployment SolutionLog on to the target computer using the Domain Name\Administrator account.

Option I: Manually Deploy a PCT Package

1. Log on to the target computer using the Domain Name\Administrator account.
2. Using the following steps, browse to the folder containing the Personality Package you just edited.
 - a. Click **Start > Run**.
 - b. Type \\DServ\Express\PCT\MyPackages in the Open field.
 - c. Click **OK**.
3. Run the Personality Package manually by double-clicking on that ComputerName.exe package. The Personality Migration Wizard dialog appears.
4. Click **Next**.
5. Click **Finish**.
6. Click **Begin** to start the migration.
7. Answer **Yes to All** for all remaining prompts.
8. After the package has been deployed, click **OK**.
9. Click **Finish** to restart the computer.
10. After the computer has restarted, log on as the Domain Name\Administrator user and verify that the migration completed successfully. Look for the following:
 - a. Confirm that configuration settings were applied.
 - b. Confirm that any files and folders were all created.

Option II: Use Tokens to Deploy a PCT Package

In this part of the exercise you will create a Deployment job to deploy Personality Packages. This job will use an Altiris token to locate the correct Personality Package to deploy. This allows one job to be deployed to many computers.

1. From the Deployment Console, create a new job in your My Jobs\PCT folder named Deploy PCT.
2. Add a Distribute Personality task to your Deploy PCT job and configure it as follows:
 - a. Name: **\\DSServer\Express\PCT\MyPackages\%COMPNAME%.exe**
 - b. Additional command-line switches: Type **-qm -r:%COMPNAME%.exe**. The -r switch creates an undo package.
3. Click **Finish**.
4. Click **Yes** to the warning prompt.
5. Schedule the Deploy PCT job to run immediately on the target computers. Because the token, %COMPNAME%, was used in the file name the single Deployment job will locate and deploy the appropriate package for each computer.
6. Verify that the packages were deployed.

Step 5: Assemble and Automate

Now that all of the required files and tasks have been built and tested, you need to encapsulate them into a Deployment Server job sequence. This ensures that when one task completes, the next is triggered automatically. The migration process will include:

- ◆ Capture personality settings (using the template built in Step 4)
- ◆ Deploy the OS image (using the image built in Step 2)
- ◆ Install required applications (using the applications prepared in Step 3)
- ◆ Restore personality settings

The Deployment Server Console provides a Job Wizard that will simplify this step.

1. In the Deployment Server Console, go to the File menu and choose **New > Job Wizard**.
2. Choose **Migrate computers** and give the job a name.
3. If you are upgrading hardware as part of your migration process, choose **Migrate one computer to another separate computer**.
4. If you are performing an in-place migration, choose **Migrate the same computer to another operating system**.
5. Enable the option **Install software packages prior to applying the personality on the destination computer** and click **Next**.
6. If you chose to migrate to separate computers:
 - a. Select all the computers that you will be migrating from and click **Next**.
 - b. Select all the computers that you will be migrating to and click **Next**.
 - c. At the **Associate destination computers** page, click each source computer listed and select its destination computer from the list.
 - d. When you are done associating source and destination computers, click **Next**.

Capture Personality Settings

This process utilizes the the template built in Step 4.

1. At the **Capture Personality Settings** page, select the personality template file built in step 4 of this document.
2. Enter a UNC path to store the package such as "\\%DSSERVER%\eXpress\PCT\Packages". You may use Deployment Server Tokens in the UNC path. If you are performing in-place migration and wish to store the personality package on the client computer's hard drive, specify the path "C:\Preserve"
3. Enter the User name and Password of a domain account that has Administrative privileges on the client computers and read/write access to the package location.
4. Click **Next** twice.

Deploy The OS Image

This process utilizes the image built in Step 2.

1. At the **Disk Image Source** page, enter the path to the image file created in step 2 of this document. For example, [\\%DSSERVER%\eXpress\Images\Win7.img](#).
2. If you use Deployment Server Tokens (as shown) in the UNC path, enable the option **Disable image path validation**.
3. If you are performing in-place migration and wish to store the personality package on the client computer's hard drive, type the following in **Additional Parameters**: -PRESERVE=C:\Preserve\
4. Click **Next**.
5. At the **Schedule Job** page, select **Leave job unscheduled at this time**, and click **Finish**.
This will create two jobs one labeled "Capture" and the other "Distribute".
6. Select the Distribute job and double-click the Distribute Disk Image task.
7. Disable the option **Boot to production to complete configuration task** and click **Finish**.
8. If additional drivers will be required to successfully deploy Windows 7 to your computers, add the Hardware Independent Imaging tasks explained in [Altiris KB Article 48891](#).

Install Required Applications

This process utilizes the applications prepared in Step 3.

1. Select the Distribute job. For each application you wish to install as part of the migration process, do the following:
2. Click **Add > Distribute Software**.
3. Enter the UNC path to the application installer (EXE or MSI), such as
"\\%DSSERVER%\eXpress\Applications\installer.exe". You may use Deployment Server Tokens (as shown) in the UNC path.
4. Click **Advanced**, choose **Run directly from file source**, specify the User name and Password of an account that has Administrative privileges on the client computers and read/write access to the eXpress share, and click **OK**.
5. Under **Additional command-line switches**, provide any command-line switches required to perform a silent install (as verified in step 3).
6. Click **Finish**.

Restore Personality Settings

The Job Wizard created a personality restore task for you. At this point, all you need to do is make sure the task responsible for restoring personality settings is the last one in the job. It is the Install Package task referencing %COMPNAME%.exe.

7 Steps to Windows 7

Migrating with Altiris™ Deployment Solution 6.9 SP3 from Symantec

When you are ready to perform the migration, you will first select the Capture job, right-click the source computer(s) you want to migrate from, and choose **Start Now**. When that is finished, you will then select the Distribute job, right-click the appropriate destination computer(s) and choose **Start Now**.

Execute and Report

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

Step 6: Migrate Systems

Before you can successfully migrate on a large scale, you need to know what is in front of you. Gathering real information about your hardware, applications, and security helps you determine when to make the move and what resources are required. Now you've done all the planning, you're ready to test and adjust your processes for deployment. In this step, you will:

- ◆ Position any servers purchased as part of the deployment plan in Step 1
- ◆ Make any required network adjustments, such as enabling multicasting
- ◆ Identify test candidates
- ◆ Document test cases
- ◆ Create a phased pilot
- ◆ Perform Migration

Position Any Servers Purchased as Part of the Deployment Plan in Step 1

Deployment Server can utilize network shares to provide local file sources to client computers. These shares should be hosted on a Windows server. The share content will need to be synchronized between all these servers so that the required files are always available to all clients. You will need to have the same share name on all servers, including the Deployment Server. You may name this share anything you like, but we will refer to it having the name "Deployment".

On all servers, including Deployment Server, determine a location with free space to hold all your images, personality packages, software packages, etc and plenty of room to grow. Create a directory named "Deployment" and share this directory as "Deployment". Once you have done this, you will need to move these files into the "Deployment" share of your Deployment Server.

Security access needs to be opened where endpoint clients can access the file shares to either download or upload files. If a client is capturing an image it needs to also have upload and perhaps overwrite access to the share. Having a security user that has access to the Deployment Server's main "eXpress" share, as well each package server's share is recommended. This user can be a domain user account (not necessarily a domain administrator) or a local Windows system account. If this is a local account make sure that all remote systems have the same login credentials with this account.

Now you need to replicate these files to your other servers. Deployment Server does not automatically replicate files between servers; you will need to manage this replication yourself. File replication with Deployment Server will involve large files (such as images), and a large number of smaller files (such as drivers and software installers). Designing a good method to replicate these files across a WAN in an automated method can be complex and challenging. Two suggested methods to replicate these files are to use Altiris Package Servers or Microsoft RichCopy.

Replicate files using Altiris Package Servers - The recommended method of replicating files between various file shares across a WAN environment is using Altiris Notification Server with package servers. When a package on the central Notification Server is updated it will automatically update all remote package server files with any updated files. One other advantage with Notification Server's package servers is that they can use network throttling so that WAN network links will not be overloaded with large amounts of traffic. For more details on Package Replication with Notification Server see [Altiris KB Article 31779](#).

Replicate files using Microsoft RichCopy - Another option to replicate files between various file shares is to use Microsoft's RichCopy utility. Because it is more complex to configure and maintain than Package Servers, it is not recommended for large environments. See Appendix B for more information about Microsoft RichCopy.

After the files have been replicated to the appropriate network locations, you will need to modify the Deployment Solution configuration to allow jobs to pull files from their nearest server. You can use the %SITE% token to allow jobs to reference files from the nearest server in Automation and Production. This process is explained in [Altiris KB Article 17101](#). If you only need to access these files from Automation for imaging, you can use PXE Environment Variables. The use of PXE Environment Variables is explained in [Altiris KB Article 45890](#).

Make Any Required Network Adjustments, Such As Enabling Multicasting

Implement the network changes identified during assessment and evaluation. This is required to support the Deployment Solution software that will be used to automate the migration process. Consult hardware vendors for details on how to make these configuration changes to your routers, switches, etc.

Identify Test Candidates

There are several different migration approaches that you can take to identify the pilot or test candidates. These different approaches can also be used to determine the pilot phases and subsequent migration rollout. These migration approaches are the following:

- **Mass Migration**
 - Move everyone to common standard.
 - Highly manageable but allows no customization based on departments or configurations.
 - Can be expensive for the company in time and resources.
 - Very few companies take this type of approach to migrations.
- **Batch Migration**
 - Maintain small set of standard configurations.
 - Batch can be based on department or similar job functions.
 - Combination of hardware refresh and re-imaging.
 - Good cost/manageability compromise.
 - About half of the companies take this approach.
- **Gradual Migration**
 - Migrate on hardware refresh schedule.
 - Lower up-front cost.
 - Can be challenging to manage.

Identify test candidates that satisfy the migration approach you will be using.

Document Test Cases

Identify the expected outcome of the migration job. A few things you will want to consider are:

- 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, create and document test cases that will verify the success of all migration scenarios. Organize these into a test matrix to use for project approval and tracking.

Create a Phased Pilot

After you have thoroughly tested the entire migration process on a single computer, you should conduct a pilot migration with a small group of users. Select the target group carefully, we recommend that you run the first pilot on a small IT group that has been involved with the overall migration project. Picking the IT users allows you to have a group of users that are able to understand if there is problem and rapidly provide feedback to the project team.

After Phase 1 migration is performed, verify that all data and settings have migrated as expected to the target group. A pilot migration also gives you an opportunity to test your overall processes. Once you have determined that the pilot migration is successful, you are ready to move to the next phase of the pilot.

Phase 2 involves migration of the larger IT department. There may be specific systems that may need to be removed from the target list of computers because those systems support critical applications or systems.

Phase 3 will be to select a department that can be migrated and moved to Windows 7. If the department is successfully migrated the pilot phase ends and the migration rollout begins.

Perform Migration

When a successful pilot has been completed it is now time to roll out the full migration. Depending on the number of total clients being managed, as well as the complexity of the environment this will need to be done in phases. There are various methods of phasing a large scale deployment, use the techniques that best fit your environment.

The Deployment process takes multiple steps, and at each step complications can arise. Often with an increase of systems being simultaneously provisioned the chance of failure or exposing a fault is magnified. When scaling the project it is important to find these issues and resolve them before you have impacted too many systems. A common approach is to start first with a migration of a small number of systems such as five to ten that are all local in a single subnet or network and complete the entire migration process on those systems. If a problem occurs at some point you might need to break apart the tasks that are contained in your migration job and run them separately on the systems being currently phased. This will allow you to analyze and identify the exact cause to the migration failure. When a smaller group has successfully

migrated then it is time to select groups at remote locations and slowly ramp up the size of computers being simultaneously migrated.

In a typical case most clients will successfully run through the migration process and complete, but some clients in the batch might fail. Depending on where the client system failed it might be possible to reassign the migration job. Clients that fail to run through the entire migration process need to be gathered together logically (not necessarily physically gathered) and then analyzed for similarities that could have caused failures. In a well planned and tested migration process the total number of failed clients should be fairly small. With proper investigation and analysis even these should be mitigated.

Step 7: Measure and Report

After a successful roll out of the automated migration, there's one last important step: post-migration reporting and analysis. Good reporting will enable your executive team to track the migration from a distance and will help you analyze aspects of migration such as:

- ◆ Total systems successfully migrated
- ◆ Problems encountered during migration
- ◆ Missing patches
- ◆ License verification

Total Systems Successfully Migrated

When a client system is successfully migrated it will report in the Deployment Server console as having completed the job with no errors. This is very easy to see visually in the Deployment Console as a green check mark next to the schedule status. You can select either an individual computer and see its job status, or you can select a job and see all clients that have been assigned that job and see their status.

This only shows the status of the overall job completion and not the status of each task individually. By default when any one task in a job fails the job will halt at that point and report back the error code or message of that failed task as the job status. This can be configured where certain error codes or messages can continue the job. Even with a failure at one point, the rest of the tasks can complete and the migration process can finish. If this is done the individual computer and tasks need to be drilled down to in the console to see these details.

The data of completed jobs is stored in the Deployment Solution database and can be queried to generate reports that can be either printed or saved to a spreadsheet. Most of the data that will be needed will be contained in the event_schedule table which contains data for all scheduled job. This data will need to be joined with the computer table to associate it with a specific computer record, and the event table to join it with a specific job name. The table status_log contains details about each individual task that was run as well. That data is very detailed and might be useful, but will increase the size of the report by a large factor.

SQL Report of completed migrations -

```
SELECT c.[name], s.[status], s.[end_time]
FROM [computer] c, [event_schedule] s, [event] e
```

7 Steps to Windows 7

Migrating with Altiris™ Deployment Solution 6.9 SP3 from Symantec

```
WHERE c.[computer_id] = s.[computer_id] AND e.[event_id] = s.[event_id]
AND e.[name] = 'Migration Job' AND s.[exit_code] = 0
```

The above query will need to have the job name of 'Migration Job' replaced with the name of the job in your Deployment console. Keep the single quotes around the name of the job in the SQL query however. Additional columns can be added to the query output such as when the job was scheduled, or when the job was started. The above query is meant as a basic report that can be expanded and modified to meet your needs. See Appendix A for more information.

Problems Encountered During Migration

The above report can be modified slightly to give a list of client systems that have run the migration job and have failed. However, in a failed job it is important to see the individual tasks to determine where it failed. The following SQL query incorporates the status_log table to gather that additional information.

```
SELECT c.[name], l.[status], l.[return_code_result] , l.[complete_time]
FROM [computer] c, [event_schedule] s, [event] e, [status_log] l
WHERE c.[computer_id] = s.[computer_id] AND e.[event_id] = s.[event_id]
AND l.[schedule_id] = s.[schedule_id]
AND e.[name] = 'Migration Job' AND s.[exit_code] <> 0
```

Once again the above query will need to be modified to contain the name of the migration job. You will also notice that the result of the first query has one result for each client where the report of failed migrations might have multiple results for a single computer record. This is because an entry is made in the status_log table each time the computer status changes. This will show every successful task and every failed task that might have modified the computer status at any time during the job execution.

Additional Windows 7 Migration Information

Listed below are some helpful places you can go to get more information about Windows 7 Migration:

The Windows 7 Resource Center has everything you need to successfully plan and execute an enterprise-wide Windows 7 migration including best practices, white papers, events, downloads, and more at <http://www.symantec.com/windows7>.

Symantec Connect, an online community where you can collaborate, learn and share ideas about Symantec solutions at <http://www.symantec.com/community>.

Appendix A

Database table computer - The computer table contains basic client computer data. The primary key for this table, and for most other associated tables where a join would be done, is computer_id. This table contains most basic computer information such as computer and domain name, operating system, serial number, UUID, asset tag. Most likely all reports created from the Deployment Solution database will use this table in their queries.

Example: Create a report of all computers names, serial numbers, and operating systems, grouped together by operating system.

```
SELECT [name], [serial_num], [os] FROM [computer] ORDER BY [os] ASC
```

Database table hardware - The hardware table contains basic hardware information, such as processor type, speed, number of processor cores. It also contains total RAM and free RAM, or how much was not in use when the client last reported inventory, and screen resolution. This table also uses the computer_id primary key that the computer table uses.

Example: Create a report of all computer model types that have Windows XP installed and have more than 1024 MB of RAM.

```
SELECT c.[model_num] FROM [computer] c
INNER JOIN [hardware] h ON c.[computer_id] = h.[computer_id]
WHERE c.[os] LIKE '%Windows XP%' AND h.[ram_total] >= 1024
```

Database table device - The device table contains all hardware devices that are attached to the client system. This includes all devices that would show up when you view Windows Device Manager on a system. You can access Windows Device Manager on a client system by right clicking on the "My Computer" icon, and select "Manage" and then select "Device Manager".

The data columns contained in this table are device name, class type, description, manufacturer, and driver. Class and driver do not use friendly names, but are instead GUIDs. These GUIDs do not link to any other table or other data in the Deployment Server database. These GUIDs are only useful if you have an understanding of them outside of the database. An example of this is if you are looking for all devices with a certain driver, you would need to find out in Windows what that driver's GUID is, and then use that directly in the query.

Example: Generate a list of all computers names that do not have a CD-ROM drive

```
SELECT [name] FROM [computer] WHERE [computer_id] NOT IN
(SELECT [computer_id] FROM [device] WHERE [name] LIKE '%CD-ROM%')
```

Database table nics - The nics table contains all network interface cards on a client computer. While some of this data is contained in the device table, there is more detailed information in the nics table. The data that is available in this table are items such as MAC address, if you are using DHCP or static IP, if the NIC is enabled or disabled, and the vendor and device IDs.

7 Steps to Windows 7 Migrating with Altiris™ Deployment Solution 6.9 SP3 from Symantec

The vendor and device ID in Microsoft Windows will display as a hexadecimal number. These numbers are stored in the Deployment Server database as a numerical value, and as such when it is queried it will show up as a decimal number. It might be necessary to convert either into our out of hexadecimal when using this data from the nics table.

Example: Create a list of all Intel network cards device names, and device ID

```
SELECT [nic_desc], [nic_device_id] FROM [nics] WHERE [nic_vendor_id] = 32902]
```

Note: The device ID for Intel devices is 0x8086. This hexadecimal number converts to 32902

Database table application - The application table contains all applications that are installed on a system that report in Windows "Add/Remove Programs" in the Control Panel. If an application installation adds a key to the following registry key it will be reported in this table:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
```

Most of the data that is contained in this registry key on each client is reported up in the application inventory and stored in this table. That includes application name, description, publisher, version, product ID. If the application developer reports this data to the registry on the client system then it will be reported in this database table. Many applications do not have complete data because they do not always populate that registry key completely. The column name will always be populated, but will sometimes contain a GUID, which isn't very reader friendly. In those cases they will usually have a description that gives the friendly name, but this is not always the case as description is an optional field for application developers.

This table will almost always contain multiple rows for each computer record since client computer will usually have multiple applications installed. The primary look up key in this table is a combination of computer_id and app_id. Most joins to this table will be done once again with the computer_id column however.

Example: Create a report of all computer names and the currently logged on user of the systems that are running Windows 7 and are using the software "Secure Endpoint" version 5.0

```
SELECT c.[computer_name], c.[logged_on_user] FROM [computer] c  
INNER JOIN [application] a ON c.[computer_id] = a.[computer_id]  
WHERE c.[os] LIKE '%Windows 7%' AND a.[description] LIKE 'Secure Endpoint'  
AND a.[version] = '5.0'
```

Appendix B

Microsoft RichCopy is a freely available utility written by Microsoft Developer Ken Tamaru. It is designed to copy large numbers of files over the network. It is optimized for high performance and supports many useful features such as Graphical User Interface and command-line interface, extended file and directory include and exclude filtering, FTP access, retain timestamp, remove files from destination that do not exist at source, verify, retry and resume failed copies, and much more.

A common scenario that begs the use of RichCopy is to replicate images, personality packages, software packages, etc. for use with Deployment Solution 6.x. Deployment Solution 6.x does not have any built-in mechanism for file replication, so RichCopy fits very nicely here. This section outlines how to replicate these files in conjunction with Deployment Solution 6.x, but you can use the process to replicate any files to any servers. It is best to have the same share name on all servers, including the Deployment Server. You may name this share anything you like, but we will refer to it having the name "Deployment".

On all servers, including Deployment Server, determine a location with free space to hold all your images, personality packages, software packages, etc. with plenty of room to grow. Create a directory named "Deployment" and share this directory as "Deployment". Once you have done this, you will need to move these files into the Deployment share of your Deployment Server.

Now you need to replicate these files to your other servers. Since Deployment Server does not automatically replicate files between servers, you will need to manage this replication yourself using Microsoft RichCopy.

On all of the servers you want to replicate the Deployment share to, download and install Microsoft RichCopy. You can find it at <http://technet.microsoft.com/en-us/magazine/2009.04.utilityspotlight.aspx>.

After you have installed it, you will need to determine the command-line parameters you will be using as described in the following sections.

1. Open the RichCopy Graphical User Interface.
2. Enable advanced options by clicking the **View Menu**, then selecting **Advanced**.
3. Next click the **Option** button.
4. In the "Overview" page, enable all of the options you want for the copy. We recommend the following:
 - a. **Default Source Path:** [\\DSSERVER\Deployment](#).
Replace DSSERVER with the name of your Deployment Server.
 - b. **Default Destination Path:** D:\Deployment.
Enter the local path to your Deployment Share here.
 - c. **Purge.**
Enabling this option will delete any file from the destination directory that does not exist in the source directory. This makes cleanup of unused files much easier, you will only need to delete the file from the source server and the deletion will be replicated down when the scheduled replication occurs.
 - d. **Verify** (Optional)
If you don't mind the replication taking longer, enable the Verify option to ensure that the data files preserve their integrity.
 - e. **Ignore READ-ONLY flag**
Enabling this option will allow read-only files to be overwritten.
 - f. **Copy if Availability in Destination:** Not exist
Enabling this option will copy files that exist in the source that do not exist in the destination.
 - g. **Copy if File size is:** Different
Enabling this option will copy files where the size of the source file is different than the size of the destination file.
 - h. **Copy if Time stamps:** Updated
Enabling this option will copy files where the time stamp of the source file is newer than the time stamp of the destination file.
 - i. **Date/Time type:** Last write
Enabling this option will base the time stamp comparison on the last write time.
5. In the **File attributes, Error Handling** page, specify the attributes and security information you want to copy. we recommend the following:
 - a. **File attributes**
Enabling this option will set the file attributes of the destination file to match the file attributes of the source file.
 - b. **Time stamp**
Enabling this option will set the time stamps of the destination file to match the time stamps of the source file.
 - c. **Discretionary Access Control List**
Enabling this option will set the Discretionary Access Control List of the destination file to match the Discretionary Access Control List of the source file.
 - d. **Group**
Enabling this option will set the security group information of the destination file to match the security group

information of the source file.

f. Owner

Enabling this option will set the owner user account of the destination file to match the owner user account of the source file.

g. System Access Control List

Enabling this option will set the System Access Control List of the destination file to match the System Access Control List of the source file.

6. Go to the **Others** page, select the Command line parameters, and copy them to the clipboard. You will use these later. You might want to save them in a text file.
7. If you want to save these settings to a file for reference later, Click **OK**, go to the **File** menu, choose **Save As**, give the file a name, and click **Save**.
8. Close RichCopy.

Now that you have the command-line arguments that you need, you can set up a scheduled task to perform the replication. On all of the servers you want to replicate the Deployment share to, open the **Control Panel**, open **Scheduled Tasks**, and create a new Scheduled Task with the following settings:

1. Give it any name you want, such as "Replicate Deployment Share"
2. Use an account that has read/write NTFS and Share permissions to the Deployment share on the Deployment Server and local server.
3. Run whether user is logged on or not.
Make sure the password is stored with the task so it can access network resources.
4. For the program to run, choose "C:\Program Files\Microsoft Rich Tools\RichCopy 4.0\RichCopy.exe" on a 32-bit server or "C:\Program Files (x86)\Microsoft Rich Tools\RichCopy 4.0\RichCopy64.exe" on a 64-bit server.
5. Add the command-line parameters that you copied to the clipboard earlier.
6. Schedule the job to run once a day or multiple times per day. Since RichCopy only replicates files that have changed, there is less risk of scheduling multiple times per day because most of the time the schedule kicks off, no files will be copied and occasionally one or two will.

Now all you need to do is manually run the replication command the first time or wait for the schedule to kick off. Your servers will all maintain a copy of the Deployment share from your Deployment Server.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
11/2009 20719035