WINDOWS 10 MIGRATION

Best practices and common pitfalls to avoid when upgrading to Windows 10

WHITE PAPER
Table of Contents
Deploying Windows 10 with Deployment Solution or Ghost Solution Suite ......................................................... 3
Approaching Windows 10 ...................................................................................................................................... 4
  What makes Windows 10 different from other OS deployments? .............................................................. 4
  Internet Explorer 11 compatibility .................................................................................................................. 4
  Windows 10 Versions ..................................................................................................................................... 5
  Windows as a Service (Branches) ..................................................................................................................... 5
  Considerations when imaging/upgrading to Windows 10 ............................................................................ 6
  Methods for upgrading .................................................................................................................................. 7
  Windows in-place upgrade path ...................................................................................................................... 7
  Upgrading through re-image .......................................................................................................................... 7
  Hardware Independent Imaging and best practices ....................................................................................... 8
  Driver Management ........................................................................................................................................ 8
  Using DISM for Driver Management ........................................................................................................... 9
  Determining the model name for DISM folder structure ........................................................................... 9
  A method for securing a mapped drive in PE ............................................................................................... 9
  Utilizing the secured credentials .................................................................................................................. 10
  Thin vs. Thick images ................................................................................................................................... 11
  Special considerations when preparing Windows 10 for imaging ............................................................... 12
  Pre-Image preparations ................................................................................................................................ 12
  Disabling Windows Update ........................................................................................................................... 13
  Enabling Windows Update ............................................................................................................................. 14
  Making use of it all – how to prepare a reference image ............................................................................... 14
  Approach used for capturing and deploying standard images with Deployment Solution .......................... 16
  Create an image of the source computer ....................................................................................................... 16
  Deploy image on the target computer ........................................................................................................... 17
  Approach used for capturing and deploying standard images with Ghost Solution Suite ...................... 18
  Create an image of the source computer ....................................................................................................... 18
  Deploy image on the target computer ........................................................................................................... 19
  Configuring Windows 10 Source Packages ................................................................................................. 21
  Assessing Windows 10 readiness .................................................................................................................. 23
  Running the Windows 10 readiness report ................................................................................................... 24
  Running the Windows 10 Setup Readiness Check ....................................................................................... 24

©2017 Symantec — All rights reserved
Sample Jobs for IT Management Suite (Deployment Solution) ............................................................... 26
Capture Job Sequence ......................................................................................................................... 27
Prepare Win10 for Image capture task .............................................................................................. 29
Create Win10 Image task .................................................................................................................... 30
Boot to Production task ..................................................................................................................... 30
Capturing and deploying user data with PC Transplant (PCT) ............................................................ 31
Deploy Job Sequence with PC Transplant .......................................................................................... 32
Capture Personality from Windows ................................................................................................... 32
Boot to PXE ....................................................................................................................................... 33
Deploy Windows 10 Image .................................................................................................................. 33
Boot to Production ............................................................................................................................. 35
Distribute Personality Windows 7 Client to Windows 10 .................................................................... 35
SCR – Enable Windows Update ......................................................................................................... 36
Deploy Job Sequence without PC Transplant ....................................................................................... 36
Boot to PXE ....................................................................................................................................... 37
Deploy Windows 10 Image .................................................................................................................. 37
Boot to Production ............................................................................................................................. 39
SCR – Enable Windows Update ......................................................................................................... 39
Windows In-Place Upgrade Job Sequence .......................................................................................... 40
Sample Jobs for Ghost Solution Suite ............................................................................................... 42
Capture Image Job Sequence ............................................................................................................. 42
Deploy Image with PC Transplant Job Sequence .............................................................................. 43
Capture Personality ............................................................................................................................ 44
Deploy Disk Image .............................................................................................................................. 45
Deploy Personality .............................................................................................................................. 47
Deploy Image without PC Transplant Job Sequence .......................................................................... 48
Appendix: SCR - DISM Driver Injection with PWL Task ...................................................................... 49

Resources & Links .............................................................................................................................. 51
Deploying Windows 10 with Deployment Solution or Ghost Solution Suite

This purpose of this whitepaper is to give you a head start in deploying Windows 10 within your organization. It covers the background of Windows 10, including best practices and common pitfalls and how to perform an upgrade to Windows 10 with Deployment Solution or Ghost Solution Suite.

There are three main ways to upgrade to Windows 10 including;

- In-place upgrade, in which you upgrade directly from "within" Windows 7, 8, or 8.1 to Windows 10
- Wipe and reload, where you re-image the existing computer with or without transferring data (personality)
- Replace (and reload), where you replace the computer, applying a fresh image to a new computer with or without transferring data

This whitepaper covers the in-place and wipe and reload scenarios, and includes collateral such as jobs, tasks, instructions, etc., to get you started on your path to Windows 10 within your organization. Consider this a starting point in your path to success with Windows 10. You can use and modify the collateral to fit your organization’s needs and share additional wisdom, tweaks, and suggestions with the community.

To download the collateral and to join in with the community please go here: https://www.symantec.com/connect/blogs/symantec-windows-10-migration-best-practices
Approaching Windows 10

When considering Windows 10, a lot of conversations center around the new "Windows as a Service" (WaaS) model, and how the branches, feature updates, and quality updates affect managing the day-to-day requirements of this new operating system and servicing model. While this is new to Windows 10, and they are certainly important content and concepts to understand, this whitepaper seeks to only discuss and enlighten the process of getting from a previous version of Windows (such as Windows 7) to Windows 10. Check out the Symantec Endpoint Management Connect community for more information on how our other solutions (such as Patch Management and Peer to Peer distribution) are solving these problems.

At the highest level, you can migrate to Windows 10 with either a wipe and reload re-imaging process or by simply updating the operating system in place without performing any imaging. We will discuss when to choose one method over another in more detail later, and it’s possible you may want to employ both strategies in your organization.

In-place upgrades can make it easier to upgrade the operating system as it retains all the content on the computer, however application compatibility is a critically important piece to consider here. Every application must be compatible with Windows 10 after the upgrade otherwise you may find yourself with applications that don’t work and need to be cleaned up manually. In the worst cases, you may find the machine won’t boot after the upgrade. Wipe and reload is, therefore, often a good fit when application incompatibilities block a clean in-place upgrade path.

If you choose a wipe and reload strategy, you’ll need to create a standard or gold image. In the next section we’ll discuss the basics and best practices for creating a standard image that can be used for all of your computers. We call this a Hardware Independent Image (HII) and include a process to handle driver injection. For those already familiar with this process on older operating systems, be aware that the introduction of Windows 10 requires several new steps to be taken.

What makes Windows 10 different from other OS deployments?
Windows 10 brings quite a few changes to commonly held views of how to best manage and handle Windows systems.

Internet Explorer 11 compatibility
As of January 12th, 2016 Microsoft effectively ended support for all versions of Interest Explorer (IE) older than version 11. IE 11 is supported on Windows 7, 8.1, and 10. As you may have already experienced, website and tool compatibility across web browsers can often be show stoppers, delaying upgrades for both IE and Windows versions.
To head off such troubles, we recommend you deploy IE 11 in your environment prior to upgrading endpoints to Windows 10. This way you can discover and address all compatibility issues first and it will make the transition to Windows 10 smoother since IE 11 is native to Windows 10.

**Windows 10 Versions**

Here’s an overview of the different Windows 10 versions:

**Windows Home**: Home, as the name implies, is most often found on laptop and desktops sold through brick and mortar and online retailers who are targeting the consumer market. Home is not a good fit for businesses as it lacks most of the features needed for businesses including NO ability to join a Windows 10 Home computer to a domain.
- Home will rarely be seen in business situations; however, if you adopt a BYOD strategy be aware of Home’s shortcomings.

**Windows Pro**: Pro is one of two versions of Windows 10 found in a business setting. It can also be found on some consumer grade laptops. Pro is typically aimed at small to medium size businesses. If you do adopt a BYOD model, Pro would be the OS of choice over Home. With Pro, you can join those devices to your domain and manage system updates.

**Windows Enterprise**: The Enterprise edition of Windows 10 includes every feature of Pro plus additional features for greater control of your managed endpoints including customizing and locking down the user experience to create a more unified experience across the company. Enterprise is also the only version of Windows that can be put into the LTSB branch which will be explained in the next section.

**Windows as a Service (Branches)**

With the release of Windows 10, Microsoft is changing their model for delivering an OS and how it is updated. Windows 10 is considered a platform on which Microsoft can build upon for many years via feature updates that are released on a regular schedule. This moves away from a model where customers are waiting years between operating systems and where updates are primarily to patch security holes instead of bringing new technology to the OS.

Which servicing branch you choose, affects and is impacted by the version of Windows 10 you have installed (Pro or Enterprise) and how often you want to receive new features.

**Current Branch (CB)**

The Current Branch (CB) is where all new features become available immediately after release by Microsoft. All consumer systems receive these updates upon release. The CB only supports the most recent build of Windows 10 at one time. For example, Windows 10 was on originally build 1511 but more recently is updated
to build 1607. Any user would have to apply the update to upgrade from 1511 to 1607 to then receive the monthly patch rollouts for Windows 10.

- Windows Home can only receive updates via the Current Branch push from Microsoft itself. Current Branch can also be applied to Pro and Enterprise Systems.

**Current Branch for Business**

Once an update has been released to the Current Branch, Microsoft gathers feedback for approximately four months and makes any fixes to the build before moving it into the Current Branch for Business (CBB). Most companies will place themselves in the CBB as it gives them some additional comfort that a new release has been vetted and reviewed for four months before a company begins to roll it out internally.

- Current Branch for Business is available in both Pro and Enterprise versions of Windows 10.
- Current Branch for Business can support up to two builds, for example 1511 and 1607.

**Long-Term Servicing Branch**

This branch is specifically for system critical computers that need to be very stable and mostly unchanged. These computers will receive the monthly security updates but will not receive the feature updates that release roughly twice a year.

- Long-Term Servicing Branch (LTSB) is only available within Windows 10 Enterprise. If a business has deployed Pro and later determines that some systems need to run Enterprise, those systems can utilize an in-place upgrade to Enterprise.

**Considerations when imaging/upgrading to Windows 10**

An important consideration is whether to upgrade Windows 10 in-place or to image it as part of the upgrade/refresh strategy. In-place upgrading can be performed with Managed Software Delivery (Client Management Suite) or a Deliver Software task in Ghost Solution Suite. It simply requires copying the content from the Windows 10 DVD/.iso file into a package or folder and deploying and then executing it on an endpoint. This process can also be used to execute some of the pre-check and upgrade validation capabilities.

For those looking to adopt a new tool for performing the in-place upgrade, the Managed Software Delivery capability in Client Management Suite is probably best suited to the task due to the in-built package distribution infrastructure. Ghost Solution Suite is perfectly capable of performing the same task; however, in a distributed environment, you should also consider the size of the data files that you’ll be moving around your organization.

To perform the re-imaging tasks, both Deployment Solution and Ghost Solution Suite are equally well suited to the task, with Ghost Solution Suite taking a more tactical approach and Deployment Solution being a better fit for larger and more distributed environments.
Methods for upgrading

Windows in-place upgrade path

Requirements
In order to perform an in-place upgrade, you’ll need the Windows 10 ISO file. It should be deployed using the Managed Software Delivery jobs, which will give you better management and reporting on systems that have the update and those that don’t.

Benefits
Some of the key benefits to performing this method of upgrade are:

- Preserve all data settings (app and drivers),
- Install (Standard)OS image
- Restore everything to the way it was
- Reduce up front testing and deployment preparation. Also, the file size is generally smaller as it’s the default OS media, no applications.
- Choice of rollback options

Drawbacks

- Compatibility issues with third-party disk encryption (Bitlocker is supported, whereas products such as Symantec Endpoint Encryption require additional workarounds in place, see SymWISE KB HOWTO125003, and some cannot support an in-place upgrade at all).
- Application compatibility may not be fully vetted. It’s entirely possible unknown app compatibility issues will only arise after the upgrade to the newer version of Windows 10.
- Any application upgrades that are required, either for compatibility or as part of a standard companywide upgrade, need to be executed pre-or post-upgrade. If you perform a wipe and re-image, these steps can be achieved simultaneously.

Upgrading through re-image

Requirements
For a complete re-image to occur, there must be a fully captured and custom image. Whether this is thin, thick, or a hybrid image approach is entirely up to the organization’s needs. Drivers are needed to complete the pre-boot loading of the OS and post-image process for keyboards, language packs, video, and sound.

Benefits

- Creating a full image allows imaging bare metal systems
- Provides a fully standardized system standard across the environment
- If BIOS to UEFI changes need to be made, applying an image is the best way to handle these changes
- Application upgrades can be achieved with little to no extra overhead

©2017 Symantec — All rights reserved
Drawbacks

- When a system is re-imaged, user data is not preserved by default as it is with an in-place upgrade. A tool such as PCTransplant, which is included with both Deployment Solution and Ghost Solution Suite, must be utilized to ensure user data is captured and deployed to the newly imaged systems.
- If any custom device drivers are required they must be installed on the machine.
- All applications that the user requires must be part of the image or be re-installed onto the system before the machine can be returned to the end user.

Hardware Independent Imaging and best practices

Hardware Independent Images (HIIs) enable organizations to capture one operating system image, and later deploy the same image to multiple machine makes and models across the organization. This is accomplished by first capturing an image that is as generic and light on drivers as possible. This image is then deployed to other computers, with drivers specific to the hardware injected as part of the process.

Many organizations would previously have had one operating system image captured for every unique make or model of computers in use. This approach takes an exponential amount of effort and disk space when compared with hardware independent solutions used in both IT Management Suite and Ghost Solution Suite. Hardware independent OS deployment solutions have existed in previous versions of Symantec products, however, with recent enhancements such as Driver Tagging, customers can more precisely control which drivers are installed for a given model. Symantec has developed Driver Tagging to specifically address the needs of newer UEFI devices with increasingly unique and challenging driver requirements.

Driver Management

Part of the imaging process will involve activating a network driver during PXE Boot as well as driver injection for post-image processing. DeployAnywhere, which is built into Deployment Solution and Ghost Solution Suite, allows for driver management through an easy-to-use interface. This is great for smaller environments where a limited amount of hardware models can be better managed. When working with a larger selection of hardware models, it can be a strain to keep the similar drivers from interfering with the selection process, especially if they contain the same name and SUBSYS information. An example of this is often seen with Intel LM network cards, where many different computer models utilize the same type of Intel LM network card, but multiple revisions require new or different network driver sets.

The alternative to DeployAnywhere is to utilize DISM to perform driver injection during the WinPE process. Utilizing DISM offers a scripted approach for distinct model selection and driver injection. The benefits of utilizing DISM is that with a simple script, we can determine the specific model and install drivers meant just for this model. This often allows for a simpler method of updating drivers, removing drivers from older models, and deploying securely when multiple hardware models exist.
Using DISM for Driver Management

Using DISM requires creating a shared folder that can be mapped as part of the script. In the attached collateral `\ServerName\DISM\Drivers` is utilized as the share location. This folder will need to be created, or the script modified, to direct to another current shared folder. Once the share is created, you need to download the latest drivers from your vendor and extract them to the specific subfolders for the models you will be deploying. The script will then map to the share and utilize the folder structure to match and scan for the appropriate drivers to inject into Windows.

Determining the model name for DISM folder structure

To determine the model name of a computer run the following command:

```
wmic path win32_computersystem get model /Value
```

An example of the output might be “Inspiron 15 3000”. You would then create a subfolder `\ServerName\DISMDriver\Win10\Inspiron 15 3000` and copy the appropriate drivers for this computer into the subfolder. When DISM performs the scan it will scan subfolders, so it is perfectly fine to create multiple subfolders within the Inspiron 15 3000 folder structure.

A method for securing a mapped drive in PE

The provided collateral utilizes a script that requires mapping to a share. To do this within a script, it’s generally necessary to provide a username and password. Entering passwords into script files or in clear text is considered a bad security practice and risks exposing the password. To address this it is recommended to use a utility called `loginw` to reduce the risk of password exposure. The utility allows storing a password in a secure file format (.pwl) and using this to perform credential validation.

The `loginw` tool has four modes. We will be focusing on the Generate and Authenticate modes. The Generate mode allows us to generate a password file. Once we create this file, we can use the authentication mode to load the file into memory and provide the credentials we need for utilities like "net use" to connect.

The `loginw.exe` utility is part of the bootwiz tool included with both Ghost Solution Suite and Deployment Solution. It is located in:

```plaintext
(DS): \Program Files\Altiris\Deployment\BDC\bootwiz\Platforms\WinPE\x86\Optional\Boot as well as \\Program Files\Altiris\Deployment\BDC\bootwiz\Platforms\WinPE\x64\Optional\Boot.
(GSS): \Program Files (x86)\Altiris\eXpress\Deployment Server\Bootwiz\Platforms\Winpe10\x86\Optional\boot as well as \Program Files (x86)\Altiris\eXpress\Deployment Server\Bootwiz\Platforms\Winpe10\x64\Optional\boot
```

The tool from either location can be utilized in the examples below.
First, we need to create the PWL file that will store the account credentials.

Enter the following command to create the PWL file:
```
loginw.exe -g UserName(withoutDomain):Password -f FileName.pwl
```
Example: `loginw.exe -g imguser:P@ssword123 -f symcPWLfile.pwl`

Next, we need to add the PWL file into our boot image so we can load it into memory before mapping network drives that would require a password. This requires copying the PWL file into the template directory, then rebuilding our Preboot Media.

```
(DS): \Program Files\Altiris\Deployment\BDC\bootwiz\oem\DS\winpe\x86\Base and \Program Files\Altiris\Deployment\BDC\bootwiz\oem\DS\winpe\x64\Base
(GSS): \Program Files (x86)\Altiris\eXpress\Deployment Server\Bootwiz\Platforms\Winpe10\x86\Templates and \Program Files (x86)\Altiris\eXpress\Deployment Server\Bootwiz\Platforms\Winpe10\x64\Templates
```

Finally, we need to re-create our pre-boot media:
- Redistribute BDC Package to site servers (with Symantec IT Management Suite or Deployment Solution)
- Run a Delta Update Schedule task in Resource Membership Update (with ITMS/DS)
- Recreate pre-boot media.

Utilizing the secured credentials

When you load a PWL file into memory, it will pass those credentials into the next command such as a net use command. An example of how to use the PWL file with loginw and net use would be the following command line(s):

```
x:\loginw.exe -f x:\FILENAME.pwl -c SERVERNAME -d DOMAIN -t 30
net use w: \\SERVERNAME\SHARE
```

It is a requirement of the loginw.exe command that the server name is provided. We can use a variable in place of the SERVERNAME.
For example:
```
x:\loginw.exe -f x:\FILENAME.pwl -c %TASKSERVER% -d DOMAIN -t 30
net use w: \%TASKSERVER%\SHARE
```
When we have the PWL file incorporated into the preboot configuration we then can add the use of loginw to our scripts allowing for secure mapping of network drives within WinPE without exposing the password in clear text. This is how the DISM Driver Injection script performs mapping of network drives and allows for easy authentication to the shared drive.

Thin vs. Thick images

Thick images are larger images in size and contain Windows Updates, Features, Frameworks, line of business applications, productivity applications, and additional customizations. The size of the image file captured will take up a considerable amount of additional storage space. The time it takes to transport the larger images across the network will increase as well. The benefit to the thick image is that there will be fewer post-OS deployment tasks to complete, as common software will already be installed.

Thin images are images that incorporate only the necessary Windows Updates, Features, and Frameworks. The resulting image is smaller in size, and enables organizations to deploy line of business applications and common productivity applications after the OS deployment. Thin images give you flexibility to update the software products deployed to the OS easily, by adding or removing new software titles to the task sequence as needed. Due to the smaller size of thin images, they will be deployed to endpoints across the network in less time than a thick image, however, consideration must be given to the time the endpoints will spend completing post-OS deployment software installation tasks.

Hybrid images are a popular choice. Hybrid images are a thin image with commonly used applications, such as Microsoft Office, already installed. Products that are used by the majority of end users and are not often updated are great candidates to be included in a hybrid image.

Creating an easily deployable image requires many decisions to be made such as deciding on the type of image you want to create and deploy and whether it will be a thick or thin image. This will help you determine what features of the Symantec Endpoint products you can leverage to best suit your needs. If you have remote offices with limited bandwidth, a thick image may take too much bandwidth to deliver to these locations, whereas a thin image will get the image out quickly, but will need to run additional jobs and tasks to complete the full deployment process.

The industry standard is to use a Hardware Independent Image (HII) with best practice being to create a standard VM and build your OS as desired, using thin or thick methods. This allows for a quickly deployable image to any system, including any new hardware that may enter the organization.

At this point you can then design out the rest of the process. You will want to consider language packs, OS patches, and third party software (Bios updates, keyboard/mouse layouts, etc.). The Symantec tools allow you
to easily use jobs/tasks/policies as part of the OS Deployment process to deploy these packages immediately after the OS is installed. The provided example jobs will help to show you how this is achieved.

**Special considerations when preparing Windows 10 for imaging**

With Windows 10, a common pitfall occurs when updates to Windows or provisioned apps have taken place prior to capturing the image. The problem occurs when provisioned applications are present within the default Windows installation and have been automatically updated for each user upon logon.

With Windows 10, this scenario requires adding some additional steps compared to how this has been done in the past. The recommendation is that the client be freshly installed with Windows Updates disabled before attempting to run a Prepare for Image Capture (sysprep) job. To quickly check if the Windows 10 machine has been upgraded, do the following:

1.) Open Regedit.exe
2.) Check for the following key: HKEY_LOCAL_MACHINE\SYSTEM\Setup\Upgrade if this key exists your system has been upgraded.

**Note:** This is the current method for imaging Windows 8, Windows 8.1, and Windows 10 clients. This method will remove all Windows Store apps from the operating system image file so a Ghost image can be made of the OS in a 'fresh' state.

**Note:** To prevent Windows Store from updating apps, unplug the Internet connection or disable Automatic Updates in Audit mode before you create the image.

**Pre-Image preparations**

- Enable the default admin account (if it isn't already enabled).
- Log into machine with the Default Administrator Account.
- Create a new local Admin account. (e.g. create a new local account named ‘localadmin’ and make sure this account is a member of the local Administrators group. We will call this account local Admin from this point).
- **Delete** all other local accounts and their profiles, leaving only the default Administrator and local Admin account created in step 3, and any default disabled accounts such as the Guest account. If the Guest account was enabled and used, you must disable this account before moving forward.
- Clear installed Apps:
  - Type 'Powershell' in the search box on the taskbar, and wait for the Windows Powershell application to appear at the top.
  - Right Click 'Windows Powershell' at the top of the list and choose 'Run as Administrator'.
- In the Powershell window, type `Get-AppxPackage -AllUser | Where PublisherId -eq 8wekyb3d8bbwe | Format-List -Property PackageFullName,PackageUserInformation`  This lists the Windows 8/8.1/10 'Modern/Windows Store' apps that are installed for each user.  All of these apps except Microsoft Edge will need to be removed for each user shown
- Type 'Get-AppxPackage -AllUsers | Remove-AppxPackage'.  
  Note: This command removes the Windows store apps for the logged in user. Errors will be displayed. This is okay.
- Type 'Get-AppxPackage -AllUser | Where PublisherId -eq 8wekyb3d8bbwe | Format-List -Property PackageFullName,PackageUserInformation'  
  The user that is currently logged in will not appear in the list (except for Microsoft Edge)
- Log out of the current user and login as the next user for which Windows Store apps are installed as shown in step 5c. (e.g. If no domain accounts are installed, the user in step three will be the only user to login. If domain accounts have Windows Store apps installed to them, login as the domain account and run the process again).
- After running 'Get-AppxPackage -AllUser | Where PublisherId -eq 8wekyb3d8bbwe | Format-List -Property Package FullName,PackageUserInformation' for the last user all apps should show 'staged' except Microsoft Edge.
- Run the Prepare for Image Capture while still logged into the local Admin account created in step 3.

**Note:** For Windows 10 make sure 'Run Sysprep with Admin Credentials' is selected. The username that is supplied below the check box needs to be the same account that is currently logged into the client system. Though the UI specifies 'domain\user' put in the local computer name and user. E.g 'win10box\localadmin'

- Capture the image, then reboot back to production.
- The only account available on the source machine and any machines imaged with this image should be the local Admin you created in step one, unless rejoined to the domain using the Deploy Image task’s 'rejoin domain' field.

There are some other known problems with how the systems behave with Windows Update enabled. A workaround is to disable Windows Update before the Capture Image or Deploy Image processes begin as part of any job.

**Disabling Windows Update**

Disabling Windows Updates at the beginning of the “gold image” creation process ensures the ability to capture the image without errors. Remember to also follow the “Enabling Windows Update” steps as part of the image deployment process.

To disable Windows update, run the following commands:
- `net stop wuauserv`
- `sc config wuauserv start= disabled`

**Note:** If the Windows updates are already installed on the source computer, then Sysprep image task fails.

- Run Prepare for Image Capture task on the source computer.
- This will create an image of the source computer (Important: after deploying this image the Windows Update service should be re-enabled!).

### Enabling Windows Update

When the image is captured with the Windows Update service disabled, it will prevent the computer from installing updates. Thus, any images deployed with the Windows Update service disabled should have a task run against them that enables the Windows Update service again.

Run the following commands to enable Windows Update services on the computer on which the Windows 10 Anniversary (1607) update is deployed:

- `sc config wuauserv start= auto`
- `net start wuauserv`
- Allow the updates required for the computer to get installed, either through Patch Management or through the updates downloading from Microsoft.

### Making use of it all – how to prepare a reference image

Putting the information in the preceding sections to use requires capturing an image to deploy. With the information covered you should be in a good position to choose the version of Windows you wish to capture and deploy as well as some of the special steps necessary to successfully prepare the image for capture.

An often-used approach is utilizing a virtual machine to build the Windows 10 installation, add appropriate base applications, based on whether you prefer a thick or thin image, follow steps to customize the look and feel according to your organization’s needs, and make sure the system is fully patched including image preparation tasks and capture of the image. Using a virtual machine affords the capability of creating “snapshots”. With snapshots you get multiple benefits, the most important being that you can work around a limitation in Windows only allowing you to run sysprep a certain amount of times and quickly restore your image to a point in time, say step X where you only need to add a few patches or applications and can re-capture the image. Using physical hardware to create and capture the image means you generally should start from scratch every time.
The steps below assume using a Virtual Machine. Many different options exist such as Hyper-V, VMware and VirtualBox. Many people gravitate towards either Hyper-V or VMware (paid) while others prefer VirtualBox (free).

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create new VM</td>
<td>Create/configure a new Virtual Machine for Windows 10</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install Windows</td>
<td>Install the version of Windows 10 you wish to base your image on. Use a “clean” installation source, such as an .iso or DVD</td>
</tr>
<tr>
<td>Step 3</td>
<td>Disable Windows Update</td>
<td>Following the steps outlined earlier to disable Windows Update</td>
</tr>
<tr>
<td>Step 4</td>
<td>Take a snapshot</td>
<td>Take a snapshot of your “clean” install. This ensures you always have the option to revert to a clean install with just Windows.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Install Software Updates (patches)</td>
<td>Install all the latest software updates (patches) and/or feature updates applicable to your Windows installation. This ensures the most secure base posture of your image.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Take a snapshot</td>
<td>Take a snapshot of your “clean image with software updates”, this allows you to revert to a point where the image is both clean without additional software and also has all the latest software updates.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Install the management agent</td>
<td>Install the Symantec Management Agent (DS) and appropriate plug-ins or DAgent (Ghost Solution Suite)</td>
</tr>
<tr>
<td>Step 8</td>
<td>Take a snapshot</td>
<td>Take a snapshot of your image. This will be your “clean image, with software updates and management agent”. This is often a “base point to base image work off and can be re-used for subsequent image captures as necessary.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Install applications</td>
<td>Install any applications applicable based on your choice of thick or thin image approach. Examples include installing a base version of Office applicable to an entire organization, or just light, but often used, applications like Adobe Reader or Flash, and yet others install all possible applications (thick).</td>
</tr>
<tr>
<td>Step 10</td>
<td>Install Software Updates (patches)</td>
<td>Install all the latest software updates (patches) and/or feature updates applicable to your Windows installation.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Perform Windows customizations</td>
<td>Perform any Windows and/or application customizations to be part of your standard image.</td>
</tr>
<tr>
<td>Step 12</td>
<td>Take a snapshot</td>
<td>The last step before capturing the image is to make a last snapshot. This ensures we can restore to this point if any error or misconfiguration prevents us from successfully capturing the image.</td>
</tr>
<tr>
<td>Step 13</td>
<td>Perform image capture</td>
<td>Use your tool of choice to perform image capture. This generally involves running a “prepare for image” task followed by capturing the image of Windows from within automation (WinPE)</td>
</tr>
</tbody>
</table>

Once the image capture has been performed, keep in mind that Windows Updates was disabled in step three. It is strongly recommended to run a task after image deployment has taken place to re-enable Windows Updates. The steps to enable Windows Update are described above this section.
Approach used for capturing and deploying standard images with Deployment Solution

Within Symantec Deployment Solution, you can utilize the Capture Image Task that will create a standard Ghost Image file for the system being imaged. For example, a standard job within the console would contain the following components for capture and a second set for deployment.

Create an image of the source computer.

Table: Process for creating an image of a Windows client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Launch the Console | Launch the Symantec Management Console.  
You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following:  
http://<IP address of NS>/altiris/console |
| Step 2 | Prepare a reference computer for imaging. | Prepare the reference computer that contains the core software and settings that you want to be replicated on other computers.  
For Windows XP and Windows 2003, install the Sysprep files on the reference computer. Copy the support\tools\deploy.cab file from your Windows XP installation disk or service pack. |
| Step 3 | Create a client job for the deployment tasks in the console | To create a client job, right-click on the Deployment folder and select New > Client Job menu. By default, a job of the name New Client Job is created that you can rename appropriately.  
Navigate to the Manage > Jobs and Tasks menu of the console and create a client job for the Deployment folder.  
To create a client job, right-click on the Deployment folder and select New > Client Job menu. By default, a job of the name New Client Job is created that you can rename appropriately. |
| Step 4 | Execute the Prepare for Image capture task | Run the Prepare for Image capture task if you want to perform Sysprep imaging and use the Include DeployAnywhere for hardware independent imaging option for the Deploy Image task. The Prepare for Image capture task ensures that the captured image does not contain any hardware-dependent data. You can then deploy a hardware independent image on other computers.  
If you deploy a disk image using the Include DeployAnywhere for hardware independent imaging option and you have not performed the Prepare for Image capture task, the client computer image gets corrupted. |
### Step 5 Create an image of the client computer

Run the **Create Image** task to create the disk image of the reference computer.

You can either run the task immediately by using the **Quick Run** option of the task that you have saved, or you can schedule the task to run later on the reference computer.

---

### Deploy image on the target computer

**Table: Process for deploying an image of a Windows client computer**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Launch the Console</td>
<td>Launch the Symantec Management Console. You can launch the console either from the Start menu of the Notification Server computer or from any computer of the network. To access the console from a different computer, you must type the following: http://&lt;IP address of NS&gt;/altiris/console</td>
</tr>
<tr>
<td>2</td>
<td>Boot the client computer to Automation environment</td>
<td>Boot the client computer to Automation environment using the <strong>Boot To</strong> task.</td>
</tr>
<tr>
<td>3</td>
<td>Create a client job for the deployment tasks in the console</td>
<td>To create a client job, right-click on the <strong>Deployment</strong> folder and select <strong>New &gt; Client Job</strong> menu. By default, a job of the name <strong>New Client Job</strong> is created that you can rename appropriately. Navigate to the <strong>Manage &gt; Jobs and Tasks</strong> menu of the console and create a client job for the <strong>Deployment</strong> folder. To create a client job, right-click on the <strong>Deployment</strong> folder and select <strong>New &gt; Client Job</strong> menu. By default, a job of the name <strong>New Client Job</strong> is created that you can rename appropriately.</td>
</tr>
<tr>
<td>4</td>
<td>Deploy the image on the client computer</td>
<td>Create a <strong>Deploy Image</strong> task for the target client computers. You can specify the Sysprep-enabled image that you captured to be deployed on the target client computers. You can either execute the task immediately by using the <strong>Quick Run</strong> option of the task that you have saved, or you can schedule the task to be executed later on the reference computer.</td>
</tr>
<tr>
<td>5</td>
<td>Run DISM Driver Injection script.</td>
<td>Create a Run Script task to perform the DISM Driver Injection script. This will allow the drivers required by Windows to function and enables deploying one image to many models of computers (HII).</td>
</tr>
</tbody>
</table>
This driver injection script needs to run after the image has been deployed, but before the computer is rebooted into “Windows” where the sysprep mini-setup will perform post image preparation tasks and ingest any added drivers. This is what makes the image hardware independent.

Step 5
Boot the client computer to production environment

Boot the client computer to production environment using the Boot To task.

At this point, various options for deployment of software needed for job functions or system functionality are added as post image work.

Approach used for capturing and deploying standard images with Ghost Solution Suite

Within Ghost Solution Suite, you can utilize the Create Disk Image task that will create a standard Ghost Image file for the system being imaged. For example, a standard job within the console would contain the following components for capture and a second set for deployment.

Create an image of the source computer.

Table: Process for creating an image of a Windows client computer

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Console</td>
<td>Launch the Ghost Solution Suite console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can launch the console either from the Start menu of the Ghost Solution Suite server or from any computer on the network where you have the Ghost Solution Suite console installed.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Prepare a reference computer for imaging.</td>
<td>Prepare the reference computer that contains the core software and settings that you want to replicate on other computers.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a new job for the deployment tasks in the console</td>
<td>To create a client job, right-click on the Jobs folder, any of its subdirectories or create a new folder, then select New Job. By default, a job of the name New Job ## is created that you can rename appropriately.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Now select the newly created job and continue with the steps below.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create the deployment capture task(s)</td>
<td>On the new job click the Add &gt;&gt; button to bring up a list of task types, then select Create Disk Image.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On the Create Disk Image configure the image capture properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set the imaging tool to Symantec Ghost (*.gho)</td>
</tr>
</tbody>
</table>
Step 5 | Create an image of the client computer | Run the **New Job** with the Create Disk Image task to create the disk image of the reference computer.

You can either run the task immediately or you can schedule the task to run later on the reference computer.

---

**Deploy image on the target computer**

**Table: Process for deploying an image of a Windows client computer**

| Step 1 | Launch the Console | Launch the Ghost Solution Suite console.

You can launch the console either from the Start menu of the Ghost Solution Suite server or from any computer on the network where you have the Ghost Solution Suite console installed.

---
<table>
<thead>
<tr>
<th>Step 2</th>
<th>Create a client job for the deployment tasks in the console</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To create a client job, right-click on the Jobs folder, any of its subdirectories or create a new folder, then select New Job. By default, a job of the name New Job ## is created that you can rename appropriately. Now select the newly created job and continue with the steps below.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Create the deployment task(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On the new job click the Add &gt;&gt; button to bring up a list of task types, then select Distribute Disk Image. On the Distribute Disk Image configure the image deployment properties. Set the location and properties of the image by clicking Select Options. Keep Use Ghost Solution Suite Server share Specify the image path using the dialog. Example above; .\Images\Win10Enterprise_x64\Win10Ent_x64_Jun5-17_01.gho. Hit OK Select Selected image was prepared using Sysprep, then hit Sysprep Settings. Specify the appropriate operating system Specify the appropriate product key Keep Use default answer file, unless you have a custom answer file created, then pick the option Use the following answer file. Hit OK Select Automatically perform configuration task after completing this image task and Boot to production to complete configuration task Select Use DeployAnywhere hardware independent imaging. Select the proper automation environment under Automation pre-boot environment to select where imaging will take place within. Hit Finish to close the Distribute Disk Image dialog</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Deploy the image on the client computer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Run the New Job against the computer to be (re)imaged. If the computer is in Windows the job will reboot it into automation. Alternatively boot the computer into PXE and assign the job once the computer is visible in the Ghost Solution Suite console. You can either run the task immediately, or you can schedule the task to run later.</td>
</tr>
</tbody>
</table>
At this point, various options for deployment of software needed for job function or functionality of the system being imaged is added as post image work.

**Configuring Windows 10 Source Packages**

To perform in-place upgrades as well as utilizing the Windows 10 Setup Readiness Check, it is necessary to copy the source files for Windows 10 onto your SMP Server/Package Repository. To make it easier to use and import the collateral, the package source utilized is “a directory on the Notification Server”. This methodology is used to allow creation of “named” folders, making the import process of the collateral easier. Before utilizing the Windows 10 Readiness Check or in-place upgrade, create the following directories:

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Package Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 OS Files 32-bit (x86 1607)</td>
<td>D:\Win10Sources\Win10_1607_32bit</td>
</tr>
<tr>
<td>Windows 10 OS Files 64-bit (x64 1607)</td>
<td>D:\Win10Sources\Win10_1607_64bit</td>
</tr>
</tbody>
</table>

Replace D:\Win10Sources with the appropriate drive and directory for your environment. Mount (or otherwise access) the ISO/DVD install source for Windows 10, as listed above, and copy the contents into the individual Package Directory locations. Both will look very similar in content, although one should be 32-bit and the other 64-bit.

Once both folder structures are in place, download and extract the Software Replicator Tool. The Software Replicator tool can be found in SymWISE KB TECH166711. Then extract and launch the software replicator tool. Next, change to the “Import Software Resources” tab.
On the Import tab, browse to the location of the extracted collateral files. In this example, the directory is “C:\Users\Administrator\Desktop\Win10Whitepaper Collateral”. Check-box the two REL_ items that contain all the information needed to define the Windows 10 in-place and validation packages and command lines.

Under the “Mapping for UNC Shares, local package paths and well known root folders (like NSCap)” update the Root on Destination if necessary. Do this by selecting the line and click the “Change” button:
Once you’re satisfied with the settings, click “Import Now” to perform the import. To re-import or make sure all information was imported properly, you can uncheck “Do not import resource which already exist in NS” to overwrite any existing resources, then re-run the Import.

Assessing Windows 10 readiness
A number of different approaches are viable for assessing Windows 10 readiness. Here we present two which can be executed within the framework of Symantec Client Management Suite (Deployment Solution) and Ghost Solution Suite.

The first option is a report that validates the base hardware requirements needed to support a Windows 10 installation or upgrade. The second options involves running the Windows 10 setup.exe, which allows use of a “Scan Only” option that returns a status code indicating whether running an in-place upgrade is expected to function or known incompatibility issues are found.
Running the Windows 10 readiness report

Windows 10 doesn’t supply an out-of-the-box readiness report, so importing it from the supplied collateral is necessary. Simply download the report.xml onto your Desktop and import it into the Symantec Management Console.

It doesn’t matter where you create the report, although it might make sense to store it in a location such as Reports > All Reports > Windows 10 Readiness, as seen here;

Note: The report utilizes inventory information, so a requirement for this report to be useful is that hardware inventory has been successfully and completely captured on computers included in the report logic.

Microsoft has published the following Minimum Requirements for Windows 10

<table>
<thead>
<tr>
<th>Component</th>
<th>Windows 10 32-bit (x86)</th>
<th>Windows 10 64-bit (x64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor (CPU)</td>
<td>1 Ghz or higher</td>
<td>1 Ghz or higher</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>1 Gb</td>
<td>2 Gb</td>
</tr>
<tr>
<td>Hard Disk Space (HDD Free)</td>
<td>16 Gb</td>
<td>20 Gb</td>
</tr>
</tbody>
</table>

The above report shows the machines meeting the minimum requirements to support an upgrade from Windows 7 64-bit to Windows 10 64-bit.

You can review the specific requirements for Windows 10 at the following website.  

Running the Windows 10 Setup Readiness Check

Another way of performing a readiness check is by running the Windows 10 setup executable with a switch to perform a scan, rather than an install. This requires access to the full installation media/content. This isn’t recommended to be run across all computers based on the size of the media content, but it can be an extremely helpful tool if you want to validate whether a particular computer model is capable of being upgraded, or if computers with some specific set of software qualify.
To do this, a Quick-Delivery task downloads the Windows 10 payload (.iso content) and executes the setup command line to perform a readiness scan. Following this, a run script task can be utilized to collect the status information stored in a local file on the system (setupact.log) within the directory C:\$WINDOWS.~BT\Sources\Panther.

To import the tasks, go to Manage > Jobs and Tasks, then right-click and select import within the Jobs / Tasks tree. Import the TASKS – Windows 10 Whitepaper. This should result in the following three tasks being imported:

Now run the appropriate QDT (quick delivery task) against the computer you wish to validate for upgrade readiness. Once the script has run (likely returning an error/error code), run the SCR task against the same computer.

Once the SCR task has run, drill into the task details and it will display a verbose output like this:

In this instance, the 0Xc1900108 error value is caused by lack of Windows updates on the computer. Several different error codes exist. A few are covered below. Any additional error codes you experience are likely to be found and explained by a quick internet search.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xC1900210</td>
<td>No issues found (good to upgrade)</td>
</tr>
<tr>
<td>0xC1900208</td>
<td>Compatibility issues found (hard block)</td>
</tr>
<tr>
<td>0xC1900204</td>
<td>Migration choice (auto upgrade) not available (probably the wrong SKU or architecture)</td>
</tr>
<tr>
<td>0XC190020E</td>
<td>Insufficient free disk space</td>
</tr>
<tr>
<td>OXC1900200</td>
<td>Does not meet system requirements for Windows 10</td>
</tr>
</tbody>
</table>
Sample Jobs for IT Management Suite (Deployment Solution)

The following section contains sample collateral to utilize for performing Windows 10 upgrade tasks. Instructions are included for both an in-place update as well as imaging tasks to capture and deploy Windows 10. Keep in mind, the tasks themselves are fairly simple. Creating the Windows install is what takes work, practice, and patience.

Be sure to review the sections around considerations and preparation activities for imaging and decide on a thick, thin, or hybrid image. As mentioned previously, the common practice is a thin hardware independent image, where additional software is added after the image has been deployed.

Make sure you have imported the Jobs and Tasks. Navigate to Manage > Jobs and Tasks, then right click and select “Import.” Next, import the TASKS – Windows 10 Whitepaper.xml collateral file. After import you should see a folder structure like this:
Capture Job Sequence

When creating our reference image, we use the Capture Job sequence. Once the computer system we want to utilize as the gold reference image contains the apps and updates as outlined below, it’s as simple as deploying a quick job to prepare the computer for imaging. Then we’ll reboot it into the automation environment where we can perform imaging tasks and capture the image. When that it complete, we’ll boot the computer back into the production environment.
In the Create Win10 Image task, the name of the captured image is set to Win10Gold_date.gho. It is a best practice to tag the image with both the date and a version number if more than one image is created on the same day. This allows other administrators to easily distinguish the images, as the image names within the console inherit the name set within the create image task.
Prepare Win10 for Image capture task

Reminder: The “Run Sysprep with Admin credentials” should be enabled and set to the local admin account created following imaging and Deployment Solution best practices. Before running this task be sure to sign into Windows with the same account.
Create Win10 Image task

Boot to Production task

Perform this task sequence to prepare for image capture. The sequence depersonalizes the SMA and runs sysprep, reboots into automation, captures the image with Ghost, and then restarts to production. The real magic happens with the depersonalization of the Symantec Management Agent and sysprep.
Capturing and deploying user data with PC Transplant (PCT)

When deploying an image, the contents of the imaged partitions will be overwritten with the contents within the Ghost file. If you deploy a Ghost image on an existing Windows install this most often leads to data loss of users’ personal files.

Various tools exist to help and have the sole purpose of capturing data on one machine/within one install of Windows and can then transfer the captured information onto the same machine when it is re-imaged or even to a new machine – if the naming stays the same.

PC Transplant is a great way to ensure that you capture all your user’s settings before migrating to a new, fully reimaged system. The PC Transplant Template Builder lets a user define a template. A PC Transplant Template specifies which settings will be captured during a Capture Personality task. The tool has an interface like the PC Transplant 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. The Template wizard can be found at <Install Drive>\Program Files\Altiris\Deployment\PCT\Template.exe

Note: Be sure to include a password for the personality to ensure that you can deploy it onto the systems you need.
Deploy Job Sequence with PC Transplant

To deploy an image while using PC Transplant we need a sequence that first captures the personality data and stores this data in a safe place, then deploys an image onto the computer and at the end restores the personality data back.

Capture Personality from Windows

The first step is to capture the personality from Windows. This is achieved by utilizing a Capture Personality task
Boot to PXE

Next a Boot to PXE task is run. This restarts the computer and boots it into PXE. Note that this requires deployment of NBS site services. Alternatively, this can be swapped with a Boot to Automation task if automation folders are being utilized.

Deploy Windows 10 Image

After capturing the personality with PC Transplant, the gold image can be deployed.
Here we kept basic settings which generally work fine out of the box. The image previously captured, “Win10gold_date.gho” (where you should use the date and a version number) is the image selected for
deployment. Other enabled settings include the DeployAnywhere driver database and using a default auto generated system file, which will produce generic images.

Boot to Production

The Boot to Production task type reboots from automation back into the re-imaged OS.

Distribute Personality Windows 7 Client to Windows 10

Once the computer reboots into production, the post imaging (sysprep mini-setup) tasks will run. Once the computer comes out of mini-setup the personality distribution will place the captured data back.
SCR – Enable Windows Update

Finally, assuming the Windows Update service was disabled in the image creation workflow, this job will re-enable the service and ensure full functionality post-imaging.

Deploy Job Sequence without PC Transplant

For some scenarios where a net new system is being deployed, we may not need or want to deploy back any captured user settings. This job excludes both the capture and deployment of the personality, and thus appears somewhat simplified.

©2017 Symantec — All rights reserved
Boot to PXE

Next a Boot to PXE task is run. This restarts the computer and boots it into PXE. Note that this requires deployment of NBS site services. Alternatively, this can be swapped with a Boot to Automation task if automation folders are being utilized.

Deploy Windows 10 Image

After capturing the personality with PC Transplant the gold image can be deployed.

©2017 Symantec — All rights reserved
Here we kept basic settings that generally work fine out of the box. The image previously captured “Win10gold_date.gho” (where you should use the date and a version number) is the image selected for
deployment. Other enabled settings include the DeployAnywhere driver database and using a default auto-generated system file, which will produce generic images.

**Boot to Production**

The boot to production task type reboots from automation back into the re-imaged OS.

---

**SCR – Enable Windows Update**

Finally, assuming the Windows Update service was disabled in the image creation workflow this job will re-enable the service and ensure full functionality post-imaging.
Windows In-Place Upgrade Job Sequence
To perform the Windows In-Place Upgrade we need to leverage the Managed Software Delivery process. This allows us to deliver the Windows 10 payload (DVD/.iso) to endpoints, and then instruct them to perform an in-place upgrade.

The command line for running the Setup.exe is very similar the one used for the Readiness Checks, so it’s advisable to leverage two command lines on the same package for both disk space reduction and preventing duplication of packages in the environment.

The collateral includes two Managed Software Delivery Policies as well as two software resources configured for containing Windows 10 x86 and x64 payloads. Following this document these would have been imported and created when following the instructions within the Reporting and Readiness sections.

To import the Managed Software Deliveries, go to Manage > Policies > Software > Managed Software Delivery, right click, and import the POLICIES – Windows 10 Whitepaper.xml.
The command line used to perform the in-place install is the same for both 32-bit and 64-bit versions of Windows. The command line utilized is:

```
Setup.exe /auto upgrade /quiet /migratedrivers all /dynamicupdate enable /showoobe none
```

An appendix at the end of this document summarizes various sources and supporting information. For more information about the setup.exe command line options, see the “Windows Setup Command Line Options” link.

Through deploying the Managed Software Delivery, it is possible to perform an upgrade to Windows 10 without the requirement to re-image (wipe and load). You may pick one method or use multiple ones. Choose what’s right for you depending on your environment’s unique requirements.
Sample Jobs for Ghost Solution Suite

Be sure to review the sections around considerations and preparation activities for imaging, and decide on a thick, thin or hybrid image for your organization. As mentioned previously, the common practice is a thin hardware independent image, where additional software is added after the image has been deployed.

Make sure you have imported the jobs by choosing to import the GSSJobs.xml.

Capture Image Job Sequence

Capturing a base image within Ghost Solution Suite is fairly simple. Make sure to follow all the recommendations and prep work for capturing Windows 10. Once you’re ready, you can execute the image capture by running “Create Win10 Image”
Once the image is captured, we now have a gold image within the eXpress share on the Ghost Solution Suite server. As indicated above the image would reside within \hostname\eXpress\Images\Windows\Win10Gold\Win10Gold_date.gho, where date should be replaced with the current day’s date and a version number if multiple images are captured in one day.

**Deploy Image with PC Transplant Job Sequence**

Once a gold image has been created, we can utilize DeployAnywhere within Ghost Solution Suite to deploy the image as a hardware independent image, as is the option within Deployment Solution.
Capture Personality

The job sequence would first capture the personality data of the computer, then distribute the image, and lastly read and deploy the personality capture.

For PC Transplant, make sure to select the appropriate transform (.PBT) or create one using the template builder. Further ensure the passwords and user accounts provided have the appropriate access. You will need the package login to deploy the PC Transplant file.
Deploy Disk Image

Once the personality capture is completed and the file is stored on the Ghost Solution Suite server, we can re-image the computer.
Here we see the image selected as well as use of Sysprep and DeployAnywhere. This will allow an easy process of deploying an image.

©2017 Symantec — All rights reserved
Deploy Personality

After the image has been laid down on the computer, perform a transplant of the PC Transplant package back onto the computer.
Deploy Image without PC Transplant Job Sequence

Deploying an image without personality transplant essentially translates into just an image deployment job. The configuration is set to use the gold image, as well as DeployAnywhere and sysprep.

Here we see the image selected as well as use of sysprep and DeployAnywhere. This will allow an easy click-form process of deploying an image.
Appendix: SCR - DISM Driver Injection with PWL Task

@echo off
x:\\loginw.exe -f x:\FILENAME.pwl -c %TASKSERVER% -d DOMAIN -t 30
if not exist Z:\ net use Z:\ %TASKSERVER%\DISMDrivers
set LOGDIR=X:\
set LOGFL=%LOGDIR%\%COMPUTERNAME%.DriverMgmt_Script.log
echo %date% %time% Beginning Driver Script > %LOGFL%
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
REM Determine Computer Model
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
for /f "tokens=*" %%A IN ('wmic path win32_computersystem get model /Value ^| FIND ":="') DO (SET CS.%%A)
echo %date% %time% The Computer Model is %CS.Model% >> %LOGFL%
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
REM Determine Destination Drive
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
for /f "tokens=*" %%A IN ('wmic Path Win32_LogicalDisk Where "MediaType='12'" Get Name /Value ^| FIND ":="') DO (SET LD.%%A)
call:CheckFile
echo %date% %time% The Selected Windows Drive is %DRIVE% >> %LOGFL%
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
REM Check for and Set Source Driver Directory
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
set SOURCE="Z:\Win10\%CS.Model%"
if not exist %SOURCE% (Echo %date% %time% Driver Source %SOURCE% does not exist. >> %LOGFL%
Exit 0)
) else (echo %date% %time% The Driver Source is %SOURCE% >> %LOGFL%
)
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
REM Set DISM Options and inject drivers
REM :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
set DISMOPTS=/image:%DRIVE% /scratchdir:"%DRIVE%\Windows\Temp" /Add-Driver /driver:"%SOURCE%" /ForceUnsigned
set DISMOPTS=%DISMOPTS% /recurse /quiet /norestart
/logpath:"%LOGDIR%%COMPUTERNAME%.dism_drivers.log"

echo %date% %time% Starting Driver Injection using Dism >> %LOGFL%
cls
type %LOGFL%
"X:\WIndows\System32\dism.exe" %DISMOPTS%

echo Dism Command: "X:\WIndows\System32\dism.exe" %DISMOPTS% >> %LOGFL%

echo %date% %time% Dism Return Code: %ERRORLEVEL% >> %LOGFL%
cls
echo :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
type %LOGFL%
rem echo :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
rem type "%LOGDIR%%COMPUTERNAME%.dism_drivers.log"
rem pause
Exit 0
:CheckFile
if exist %LD.Name%\Windows\Tasks Set DRIVE=%LD.Name%
Echo %date% %time% DRIVE variable set to %DRIVE% >> %LOGFL%
goto:eof
Resources & Links

Symantec Windows 10 Migration Best Practices
https://www.symantec.com/connect/blogs/symantec-windows-10-migration-best-practices

Software Resource Replicator
http://www.symantec.com/docs/TECH166711

Windows 10 Upgrade and Installation Errors (error codes)

Windows 10 Setup Command Line Options

Windows 10 System Specifications & Requirements

Windows 10 Upgrade Paths

Windows 10 Upgrade Scenarios


Windows Setup Command-Line Options
https://msdn.microsoft.com/windows/hardware/commercialize/manufacture/desktop/windows-setup-command-line-options#setup_exe_exit_codes

Upgrading Encrypted Computers to Windows 10 from Earlier Versions of Windows


More Information
Visit our website
http://go.symantec.com/itms

To speak with a Product Specialist in the U.S.
Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website.

About Symantec
Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

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